Introduction and Evaluation of Attachability for Mobile IoT Routing Protocols with Markov Chain Analysis

Bardia Safaei, Hossein Taghizade, Amir Mahdi Hosseini Monazzah, Kimia Talaei, Parham Sadeghi, Aliasghar Mohammadsalehi, Jörg Henkel, and Alireza Ejlali

***Abstract*—Reliability of routing mechanisms in wireless networks is typically measured with Packet Delivery Ratio (PDR). Basically, PDR is reported with an optimistic assumption that the topology is fully constructed, and the nodes have started their packet transmission. This is despite the fact that prior to being able to transmit packets, nodes must first join the network, and then try to keep connected as much as possible. This is a key factor in the overall reliability provided by the routing protocols, especially in mobile IoT applications, where disconnections occur frequently. Nevertheless, there is a lack of appropriate metrics, which could evaluate the routing mechanisms from this perspective. Accordingly, this paper introduces attachability; a new metric for evaluating the capability of routing protocols in assisting the mobile or stationary nodes in joining, and maintaining their connections to the network. Our newly proposed metric is calculated via Markov chain analysis along with the sample frequency-based estimating technique. To evaluate attachability, we have simulated a mobile IoT infrastructure, and conducted a comprehensive set of experiments on different versions of the IPv6 Routing Protocol for Low-power and lossy networks (RPL). Based on our observations, attachability is significantly dependent on the employed metrics and path selection policies in the routing mechanisms. Among the three different versions of RPL, including the original version (ORPL), which is standardized for stationary IoT applications, and two mobility-aware versions, i.e., MARPL, and OMARPL, OMARPL showed up to 42%, and 10% of improvement in terms of attachability against ORPL, and MARPL, respectively.**

***Index Terms*—IoT, Wireless Networks, Mobility, Routing, Dependability, Reliability, Attachability, Markov Chain, RPL.**

I. Introduction

ADVENT and proliferation of miniaturized smart embedded devices, and the recent advances in their ability to be interconnected via internet-based wireless technologies have enabled the emerging paradigm of Internet of Things (IoT) [1]. IoT is a communicative infrastructure, which is able to establish Internet-based communications between numerous number of identified, short range, and resource-constrained embedded devices in relatively harsh environments with no or minimum human intervention. It has been estimated that there will be nearly nine smart devices per person at the end of 2025 [2]. Connection of this number of embedded devices in the network, necessitates the employment of resource-aware routing policies for providing a seamless connectivity and data transfer. The existing routing mechanisms, which are widely used in IoT infrastructures, are facing with many reliability-related challenges, e.g., uneven load-balance, and congestion [3]. Nevertheless, movement of the nodes in mobile IoT applications could severely intensify these issues along with creating other types of challenges, including frequent handover procedures, occurrence of inconsistencies, and imposing control overhead to the network due to maintenance of the dynamic topology [4].

All of the above mentioned issues would represent themselves in form of a reduced amount of Packet Delivery Ratio *(PDR)*. PDR has been the de-facto criterion for evaluating the reliability of routing protocols in IoT and Wireless Sensor Networks *(WSN)* [5]–[8]. PDR is reported with assuming that the topology is fully constructed, and the nodes have started their packet transmission. Nevertheless, this is an optimistic assumption, because in case of using any type of routing mechanism in the network, prior to being able to transmit the packets, nodes must first join the network based on the policies of the routing protocol, and then try to maintain their connection to it as long as possible. This issue is a key factor in the overall reliability provided by a routing protocol, and should be considered along with PDR simultaneously. Despite its importance, there does not exist any metric, which could measure this matter.

Accordingly, in this paper, we have proposed **Attachability**, a new metric for measuring the capability of routing protocols in assisting the mobile or stationary nodes in joining, and maintaining their connection to the network based on their routing policies. This newly defined metric, which is expressed in form of percentage, enables us to evaluate different routing policies, cost functions and protocols, especially in case of having mobile objects in the network. Because in mobile applications, due to the frequent movement of the nodes, providing a seamless connectivity is significantly important, and it highly depends on the employed policies of the routing mechanism. In order to calculate the amount of attachability for a certain routing mechanism, first it is required to model the connectivity behavior of the mobile nodes under the presence of the specified routing protocol as a Markov chain. Meanwhile, since the movement of the nodes are fundamentally affected by the employed mobility models,

Bardia Safaei, Hossein Taghizade, Parham Sadeghi, Aliasghar Mohammadsalehi and Alireza Ejlali are with the Department of Computer Engineering, Sharif University of Technology, Tehran 11365-11155, Iran (e-mail: bardiasafaei@sharif.edu; {htaghizade, psadeghi, mohammadsalehi}@ce.sharif.edu; ejlali@sharif.edu).

Kimia Talaei is with the Department of Computer Engineering, Universtity of Toronto, Toronto, Canada (email: ktalaei@mail.utoronto.ca)

Amir Mahdi Hosseini Monazzah is with the School of Computer Engineering, Iran University of Science and Technology, Tehran 16846-13114, Iran, and also with the School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Tehran 19538-33511, Iran (e-mail: monazzah@iust.ac.ir).

Jörg Henkel is with the Chair for Embedded Systems (CES), Karlsruhe Institute of Technology (KIT), 76131 Karlsruhe, Germany (e-mail: henkel@kit.edu).

Manuscript received x xx, xxxx; revised x xx, xxxx.

and mobile IoT applications are generally coping with severe dynamicity and fluctuations with partial or complete random attributes, the sample frequency-based estimating technique [9] must be performed to determine the rate of the transitions in the obtained Markov chain model. This will help us to mathematically formulate the attachability and calculate its value.

Despite the existence of several routing mechanisms, which could be used in IoT infrastructures, e.g., the Lightweight On-demand Ad-hoc Distance-vector routing protocol - Next Generation (LOADng) [10], or Ad-hoc On-demand Distance Vector Routing (AODV) [11], due to their weakness in providing the required level of resource consumption in such networks, in 2012, the Internet Engineering Task Force *(IETF)* introduced the IPv6 Routing Protocol for Low-power and lossy networks *(RPL)* to be adopted by IoT applications [12]. The standard version of this protocol was primarily designed for stationary IoT applications, and it was not able to support mobility. Due to the indispensable penetration of mobile IoT applications in recent years, there have been many efforts on proposing mobility-aware versions of RPL to resolve different drawbacks of its basic model [5], [13]–[17].

As part of our evaluations to measure, and compare the attachability of different routing policies, we have considered the RPL routing protocol as the underlying routing mechanism in our simulations. Based on the employed estimating technique, an extensive set of experiments have been conducted in the Cooja simulation environment [18] to gather the required data for feeding into the obtained Markov chain model for the RPL. Our attachability analysis have been performed for three different versions of RPL routing policies, i.e., the original version *(ORPL)*, which is not capable of handling the movement of the objects, and also two other mobility-aware versions of this protocol, including MARPL [16], and REFER (also known as OMARPL) [17]. In addition to different building blocks of routing policies in the protocols, e.g., trickle algorithm, objective function, neighbor table placement, and control packet management, we have shown that there exist several other network configuration characteristics, which could directly impact the amount of provided attachability by a routing protocol. Accordingly, we have considered different scenarios with varied node densities, and different mobility patterns to demonstrate our claims. Based on the experiments, it has been observed that OMARPL provides nearly 42% of more attachability against its standard version, while it also improves the amount of attachability against MARPL by more than 10%. Furthermore, our experiments have shown that among different employed mobility models, OMARPL has represented the most amount of attachability in case of employing the Boundless-Area mobility model [19] for the movement of the nodes in dense IoT networks. In addition, according to our observations, independent from the routing policy, and the movement pattern, deploying more number of nodes in the area increases the amount of provided attachability by a routing protocol.

The rest of this paper has been organized as follows: In section II, the structure of RPL, importance of Markov chain models in stochastic processes, and also the process of calculating probability distributions of the states will be explained in detail. A number of related studies corresponding to the use of Markov chain analysis in the context of dependability in IoT and WSN have been reviewed in section III .Section IV concentrates on the definition of attachability, and also explaining the process of its calculation for the RPL routing protocol. Section V is dedicated to system setup and evaluations. Finally, the paper will be concluded in section VI.

II. Preliminaries

In this section, a brief overview on the structure of RPL, its characteristics along with its downsides in confronting mobile applications, and also a number of real-world implementations will be addressed. In addition, the concept of Markov chain model and sample frequency-based estimating technique will be explained, which have been both exploited for calculating the amount of attachability in the RPL routing protocol.

A. IPv6 Routing Protocol for LLNs (RPL)

It has been estimated that every person on earth will own more than 9 smart devices at the end of 2025 [2]. This increasing trend in the number of connected smart devices and the pervasive nature of IoT applications has motivated many international organizations to concentrate on proposing a standard routing mechanism to be adopted by IoT infrastructures. A proper routing mechanism for IoT networks must comply with the resource-constrained nature of the deployed embedded devices, while it could provide flexibility and adaptability to different IoT applications. It should also support different types of traffic patterns, i.e., Point-to-Point *(P2P)*, Multi-Point-to-Point *(MP2P)*, and Point-to-Multi-Point *(P2MP)*, and provide reliable communications in the network. Accordingly, the IETF created the Routing Over Low-power and Lossy Networks *(ROLL)* working group to propose a routing mechanism, which is capable of meeting these attributes. Finally, in 2012, the group publicly announced the accomplishment of their duty and introduced the standard version of the RPL routing protocol [12].

RPL is a proactive routing protocol, which the nodes store their routing information in routing tables. Therefore, the nodes are able to promptly transmit their data to their destination(s) without requiring any route discovery procedures. Accordingly, for the sake of stability, update packets must be exchanged between the surrounding neighbors, to keep their tables updated. In RPL, nodes are organized in form of a tree-shaped structure, which is called Directed Acyclic Graph *(DAG)*. Typically, every DAG could be composed of several sink nodes. Nevertheless, RPL tries to split the network into few sub-trees with only a single sink. In this case, the tree-shape structure will be called Destination Oriented Directed Acyclic Graph *(DODAG)*. The structure of the DODAG, and the established paths between the nodes are generally dependent on the path selection policies, determined by the RPL's Objective Function *(OF)*. OF is an entity, which its duty is to optimize a single or a set of node/link metrics to meet different requirements of the intended IoT application, i.e., energy efficiency, reliability, stability, etc.

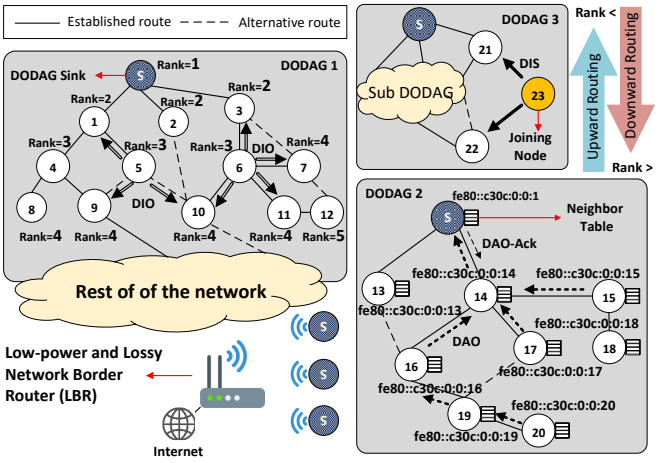


Figure 1: Structure of an RPL instance with three DODAGs.

The entire process of path selection and network maintenance in RPL is upon four Internet Control Message Protocol version 6 *(ICMPv6)* control packets. Among them, the DODAG Information Object *(DIO)* has the most pivotal role with having the responsibility of constructing the DODAG. DIO is initially broadcasted by the sink, and later it will be disseminated by the nodes to inform their neighboring nodes about the most important and updated routing-related information, such as OF, trickle timer parameters, parent table replacement policies, rank, and other configuration information required for maintaining the DODAG. Upon reception of the DIO messages, the nodes would be able to add a member of their neighboring nodes to their candidate parent set, and further choose one of them as their preferred parent [2].

It is worthy to mention that due to the limited power supply in IoT devices, the DIO messages are set to be disseminated based on a trickle mechanism, which increases the period of two consecutive transmission periods in an exponential manner [20]. Destination Information Solicitation *(DIS)* is another control message in the structure of RPL, which is transmitted by the nodes for requesting to join/rejoin a DODAG. Any member of the DODAG, who receives a DIS will send back a unicast DIO message to provide the soliciting node with the required routing information for joining the network. As it has been illustrated in Fig. 1, these two previously mentioned control packets are basically responsible for establishing upward data transmission towards the sink. Nevertheless, for the sake of P2P, and P2MP data flows, RPL is also capable of supporting downward routing via Destination Advertisement Object *(DAO)* messages. Furthermore, based on the required level of reliability in the IoT application, upon an explicit request from the transmitting node or occurrence of an error, the receiver could send back a *DAO-ACK* to the transmitter.

While RPL has been an attractive target for many industries, e.g., Cisco Resilient Mesh in smart grids (formerly known as CG-Mesh) [21], it is still coping with major flaws, especially in terms of its reliability, due to not being able to adapt with the severe fluctuations in many contemporary mobile IoT applications. Accordingly, there have been many efforts on proposing mobility-aware versions of this routing protocol [13], [14], [5]. Meanwhile, the authors in [16] have introduced a mobility-aware, and energy-efficient parent selection mechanism for IoT networks *(MARPL)*, which not only considers various node/link metrics in its structure, e.g., the euclidean distance between the moving objects, but it also employs a dynamic trickle algorithm for solving the long listen only period. In addition, an optimized version of this protocol, known as REFER (also called OMARPL) has been proposed in [17], where the authors have tried to improve its reliability with employing a new table replacement policy with restricted parent leasing time, prioritizing the connection to stationary nodes instead of mobile nodes, and also applying threshold values for triggering the handover procedure. As it will be discussed later, these two mobility-aware versions of RPL, along with its original version have been considered for conducting our attachability analysis in this paper.

B. Markov Chain Models

Exploiting state models for capturing the important aspects of systems has been a common practice in engineering, and scientific communities. Among them, Markov chains are known as a prevalent tool in computer science, which allow us to model stochastic processes that can not be modeled in a deterministic manner. Whether we use continuous or discrete sample space for the time, we could have two families of Markov chains: 1) Continuous-Time Markov Chain *(CTMC)*, and 2) Discrete-Time Markov Chain *(DTMC)*. These models are typically represented with a tuple of random variables $X(t, \zeta, \phi)$, where t belongs to the time set $T = [0, \infty)$, ζ indicates random factors of the system, and ϕ is a member of limited number of design parameters [22]. In these models, $X(t, \zeta, \phi)$ (or simply $X(t)$) represents the state of the system at time t, which should be a member of the state space S. As it has been illustrated in Fig. 2, Markov chains are composed of finite number of states (n), where every state represents a specific aspect of the system, either positive or negative. In DTMC models, the system remains in any state for exactly one unit of time before making a transition to another state, while in CTMC models, the system is allowed to stay in every state for any continuous period of time.

A stochastic process is said to be a Markov process, if it follows the Markovian property. According to (1), the Markovian property, which is also referred to as the memoryless property, indicates that the probability of being in a state in the future, only depends on being in the present state [23].

$$\begin{aligned} &Pr\{X(t+1) = s_{t+1} | X(t) = s_t, X(t-1) = s_{t-1}, ..., X(0) = s_0\} \\ &= Pr\{X(t+1) = s_{t+1} | X(t) = s_t\}, s_i \in S \end{aligned} \quad (1)$$

The continuous-time Markov chains could be simply described by two matrices. In these models, the transition of states between two consecutive points of time is expressed with a transition probability matrix (TM). Every entry of this matrix $(p_{s_i \to s_j})$ indicates the probability mass function of the system making a move from state i at time t, to state j at time $t + \Delta t$. Furthermore, as it has been represented in (2), there is an

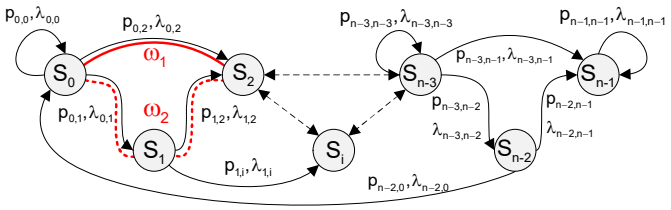


Figure 2: State diagram of a Markov chain ($\lambda_{i,j} = \lambda_{s_i \to s_j}$).

infinitesimal generator matrix (Q), which determines the rate of transitions between different states of the system $(\lambda_{s_i \to s_j})$.

$$Q = [\lambda_{s_i \to s_j}], \lambda_{s_i \to s_i} = -\sum_{j=0}^{n} \lambda_{s_i \to s_j} \tag{2}$$

In order to support the Markovain property, the time interval that the chain spends in state s_i, before moving to another state s_j, follows the exponential distribution. This interval is known as the holding time $(H_{s_i \to s_j})$, and it's average amount is obtained via $E(H_{s_i \to s_j}) = 1/\lambda_{s_i \to s_j}$. It should be also mentioned that when the system begins its operation, the initial probabilities are expressed via $I = \{I_0, I_1, ..., I_{n-1}\}$. I_i indicates the probability that the system starts from state s_i. In order to use Markov chain analysis for obtaining the transient and steady state specifications of the system, we should first estimate the transition rates for determining the generator matrix Q, which could be done through the following equation.

$$\lambda_{s_i \to s_j} = \frac{N_{s_i \to s_j}}{N_{s_i}} \quad i, j \in \{0, 2, ..., n-1\} \tag{3}$$

where $N_{s_i \to s_j}$ indicates the number of times the system performs a transition from state s_i to s_j, and N_{s_i} represents the number of transitions between two states with s_i as their starting point. Accordingly, one of the challenges that one may face in utilizing Markov chain analysis, is the calculation of $N_{s_i \to s_j}$, and N_{s_i} in situations, where the generator matrix is not known beforehand. There are several approaches for estimating these values, such as historical observations of the system states, Bayesian parameter estimation [24], survival analysis, and maximum likelihood estimation [25]. Meanwhile, many of these analytical, and statistical methods, including the Bayesian parameter estimation are complicated, and impose significant computational costs [22]. If neither of the methods are applicable to the intended system, and there exists no conditional state data, the transition rates could be determined based on the expert opinion or mechanistic-empirical models to obtain the best fit values with relatively lower precision [26], [27]. The later approach is not applicable to systems with numerous states. In this study, in order to solve our Markov model and calculate the attachability for mobile RPL-based IoT networks, we have employed the sample frequency-based estimator, which has been shown to be symptotically optimal in case of having large number of samples [28]. In this technique, which fundamentally relies on the previous observations of the system, the transition rates are achieved via conducting numerous sequential samplings from the states at uniform time intervals over a long period of time [9]. More detailed information has been provided in section IV, regarding the process of obtaining the generator matrix (Q) via sample frequency-based estimator as part of Attachability calculation.

As it has been illustrated in Fig. 2, in the state diagram of Markov chains, there may exist one or more paths (ω_i) composed of i sequential transitions towards a specific state s_ν. With keeping in mind that every transition of the chain is traversed in a single time slot, if two states are not adjacent, making a transition between them requires more than a single time step. Therefore, in order to obtain the probability of being at state s_ν at time $t + \Delta t$, all of the single-step paths, leading to s_ν must be taken into consideration. This probability is represented by $P_{s_\nu}(t + \Delta t)$, and it is calculated via (4) [29].

$$P_{s_\nu}(t + \Delta t) = \sum_{k=0}^{n} p_{s_k \to s_\nu} \times P_{s_k}(t) \tag{4}$$

After determining all of the probability equations for all of the states in form of (4), every one of them could be rewritten in form of (5), and then turned into a derivation equation. The generator matrix is usually utilized to directly determine the derivative equations for all of the states as in (6). Afterwards, the Laplace transformation will be employed to solve the differential equations, and obtain the time-dependent equations for the probability distribution of the states.

$$P_{s_\nu}(t + \Delta t) - P_{s_\nu}(t) = f(\Delta t) \times P_{s_\nu}(t) \tag{5}$$

$$[P'_{s_i}(t)]_{n \times 1} = Q_{n \times n} \times [P_{s_i}(t)]_{n \times 1}, s_i \in S \tag{6}$$

Finally, based on the type of the parameter, which is intended to be calculated, e.g., reliability, availability, or attachability, the probability function of a single state, or the sum of probability functions for a number of states will be provided as the ultimate outcome.

III. Related Studies: Markov Chains, and Dependability in Wireless Routing

Markov models have been extensively used in the context of dependability. As it will be discussed later, in addition to reliability, dependability covers a wide range of domains such as survivability, availability, maintainability, security, etc, which are all targeted in different studies. In order to provide a durable and reliable wireless communications in multi-hop mobile applications, the authors in [30] have proposed a routing mechanism, which examines the level of interference and selects the most reliable path with a Markov predictor. The authors in [31] have employed Markov chains to determine the reliability of a wireless sensor network, based on the quality of communications in a single hop between two adjacent neighbors. A two-dimensional Markov chain framework has been employed in [32] for specifying the highly complicated dynamics of mobile networks. Accordingly, a Markovian analysis has been conducted to measure important performance metrics, such as the variance of the fraction of the nodes, which have received the messages.

In many studies in the filed of routing, Markov chains are not part of the main solution, but they are mainly used for evaluations. For instance, one of the well-known medium

access control mechanisms used in IoT networks is the Time Slotted Channel Hopping *(TSCH)*. This mechanism uses time division multiple access with channel hopping, and allows several parallel communications at a time, providing reliable data delivery and efficient power consumption in a bounded latency [33]. Nevertheless, TSCH is limited in establishing global synchronization among IoT devices. Hence, the IPv6 over the Time Slotted Channel Hopping mode of IEEE 802.15.4e *(6TiSCH)* was introduced to fill the gap between the IETF low-power IPv6 communication stack (including the RPL routing protocol), and TSCH. Many studies have been carried out via Markov chain analysis to evaluate the mutual relation between RPL and 6TiSCH.

It is worthy to mention that congestion is one of the major threats towards lower PDR and lower reliability in wireless networks. Authors in [34] have used a Markov chain-based probabilistic analysis to show the high impact of various RPL-based parameters on the formation of 6TiSCH networks, due to more congestion in the minimal cell with increasing the number of nodes. Based on their observations, they have modified the RPL trickle algorithm so that sufficient routing information could be provided without congesting the minimal cell. They have also mentioned that the minimal configuration version of 6TiSCH *(6TiSCH-MC)*, underutilizes the channel resources, and imposes higher network formation time. Therefore, they have proposed autonomous allocation and scheduling of minimal cell *(TACTILE)*, and evaluated its average joining time via Markov chain analysis [35]. Furthermore, a dynamic resource management algorithm to be executed during the network bootstrap has been introduced in [36] to overcome the long network formation of 6TiSCH-MC, and sub-optimal performance of the RPL routing mechanism. In a related study, based on a Markov chain model, the impact of node mobility over a TSCH network, and the association process of the nodes is investigated [37].

One of the challenges in RPL-based 6TiSCH networks is the increment of congestion due to increment of inevitable beacon transmissions, when a new node joins the network. In order to overcome this trade-off, authors in [33], have proposed a method, in which beacon transmission interval varies with the channel congestion status during the network formation. Accordingly, Markov chain analysis has been employed to evaluate and compare the performance of this new approach with 6TiSCH-MC, and few other benchmark protocols. The interested reader is referred to [38], [39] for more similar studies. Markov chain analysis has been exploited to show that the transmission load in RPL's trickle algorithm is unevenly distributed between the nodes, i.e., some nodes (re)transmit more than others on average [40]. Accordingly, authors have come up with a novel trickle solution *(D-trickle)* that adapts a redundancy parameter to achieve higher fairness while keeping the transmission load low. On the other hand, the authors in [41] have introduced a non-cooperative gaming theory mechanism to avoid congestion with determining the optimal data rate of all the source nodes in an RPL-based network. This new approach, which is called *NGECC* has been evaluated with Markov chain analysis. In a similar study, a new method has been introduced to control congestion in the minimal cell of RPL-based 6TiSCH networks without any signaling overhead. This has been achieved with a game-theoretic solution with calculating the slot-frame window size for every node, providing an optimized transmission of control packets by the joining nodes [42]. With considering various congestion schemes for RPL-based networks, authors in [43] have proposed an effective buffer-loss estimation model based on a Markov chain queue to determine the number of packets lost at the buffers of IoT devices.

In addition to reliability, survivability is another field of study, which has been a target for employment of Markov chains. According to [44], survivability refers to the capability of an information system to fulfill its mission, in a timely manner, in the presence of faults, failures, attacks or any type of accidents. The authors in [45] have utilized CTMC to propose a quantitative model for evaluating the survivability of routing mechanisms in large-scale Mobile Ad-hoc Networks *(MANETs)* in case of facing various types of faults. The authors in [46] have studied the survivability of a wireless network, where the routing failures occur due to movement of the nodes. They have enhanced, and validated the previous studies by analysing the availability of the ad-hoc connection with the use of a Markovian model.

In disaster scenarios, localization, routing, and data delivery turns into an important issue due to the frequent displacement of mobile devices in the infrastructure-less environment. Hence, the authors in [47] have proposed an optimal-start multi-path routing, based on the hidden Markov model, which is able to forecast the future location of mobile devices based on their historical states. In addition, the hidden Markov model is used in [48] to detect misbehavior (i.e., not following the routing rules) of vehicles in Vehicular Ad-hoc Networks (VANET) based on how they are passing the data, and their traffic density distributions. Due to the importance of reliability of multi-hop forwarding in VANETs, the authors in [49] have proposed a new forwarding protocol, and modeled their protocol with Markov chains for evaluating its end-to-end success probability. The packet loss in the links could be also described by finite-state Markov chains for calculating the minimum energy packet forwarding under deadline and reliability constraints [50].

Markov models are also employed in the context of security in the routing of different WSN and IoT applications, including VANETs [51]. Markov models are known as a valuable asset for detecting cyber-attacks in the networks [22]. An analytical model based on Markov chains has been proposed for modeling the effect of black-hole attacks on opportunistic routing protocols in [52]. The authors in [53] have proposed a trust-based security extension to the Dynamic Source Routing protocol *(DSR)*, which the trustworthiness of the nodes is estimated according to their state probability based on a hidden Markov model.

Markov Decision Process *(MDP)* is also utilized in [54], [55] for providing an intelligent route planning in case of uncertainty and inconsistency in IoT networks. The authors in [56] have used a controlled finite state Markov chain to study the trade-off between PDR and resource consumption in an Opportunistic Network *(OPPNet)* with epidemic routing

mechanism. Furthermore, due to the importance of latency in OPPNets, the authors in [57] have proposed a precise latency estimation model with less complexity via Markov chains. Markov chain models have been also used as a tool in [58] for characterizing the sensitivity of E2E delay against link errors in the presence of different routing protocols. In a related study, authors in [59] have used Markov chain models to estimate the E2E delay in an RPL-based network. The authors in [60] have proposed a routing algorithm for Delay Tolerant Networks *(DTNs)* with high success rates. This algorithm labels the frequently visited places as landmarks. In this method, every node predicts its movement according to its previous landmark visits with employing an order-k Markov predictor.

IV. The Concept of Attachability

According to the literature, one of the main use-cases of Markov chains is the analysis of dependability metrics in wireless routing mechanisms, e.g., survivability, availability, and mostly reliability. Meanwhile, those studies, which have tried to focus on the reliability of routing protocols have mainly concentrated on the PDR. The PDR in a network is defined as the ratio of successfully received packets by the sink, to the total number of transmitted packets towards it by the existing nodes. However, prior to having a successful packet transmission towards the intended destinations (including the sink), a node has to satisfy the two following preconditions: 1) The node has to successfully join the network at time t, and 2) The node has to maintain its connectivity to the network while operating. Management of these issues is upon the employed routing protocol. Besides of stationary networks, where the nodes do not displace in the area, since the connectivity of the nodes to their attachment point becomes significantly more challenging in mobile networks, in this paper we have introduced *Attachability*; a new dependability metric represented with $A(t)$, which determines the capability of routing protocols in assisting the nodes for joining the mobile network, and maintaining their connection through the routing policies. We believe that attachability has a more pivotal role than PDR in determining the overall reliability of a routing mechanism. Accordingly, in order to measure the reliability of a routing algorithm, one should consider both, the PDR, and the attachability simultaneously.

Definition. 1 (Attachability)**.** A soliciting mobile node MN_k intends to join a network at time t_0; let the random variable T represent the connectivity duration of MN_k to the network after its connection. Consider the following assumptions during the $[t_0, t]$ interval:

1) MN_k shows a 100% of hardware and software reliability with no failures ($\lambda^f_{(t_0,t)} = 0$).
2) Discharge occurs due to other reasons than the routing policies, e.g., harvester or battery failure.
3) MN_k does not leave the visibility of the network (transmission range of the farthest connected node) due to its movement.

As we have indicated in (7), the attachability of a routing protocol is a function of time represented by $A_T(t)$, which is

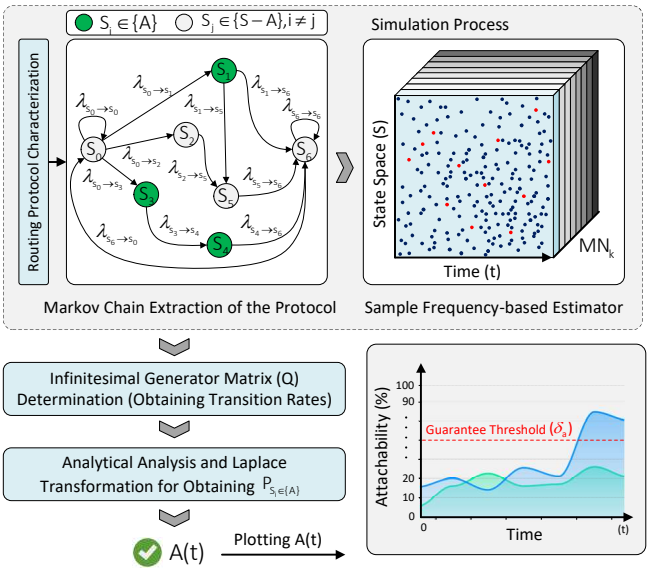


Figure 3: General Process of Calculating Attachability.

the conditional probability that a mobile device is successfully connected to the network at time t_0, and remains partially connected during $[t_0, t]$.

$$A_T(t) = Pr(T > t), t_0 < t < +\infty \tag{7}$$

According to definition of $A_T(t)$, a partial connection during $[t_0, t]$ indicates that the node is allowed to be disconnected and connected again; but in case of reaching t, the node is assumed to be permanently disconnected from the network. In order to calculate the amount of attachability for a routing mechanism in a mobile network, a series of steps should be taken. According to Fig. 3, the first step towards calculating $A(t)$ is to conduct a comprehensive study on the intended routing mechanism, and extract its characteristics. In this regard, with respect to the definition of attachability, we should first determine the tasks that are done by the protocol for establishing a connection between the mobile node, and the network. These tasks could be generally divided into two phases: *1) pre-junction*, and *2) post-junction*. The pre-junction phase is composed of tasks, which assist a node to join the network, while the post-junction phase involves a number of tasks, operated by the routing mechanism, to maintain the connectivity of a node to the network. Afterwards, the connectivity of mobile nodes to the network (under the presence of the intended protocol) could be considered as a system, and it could be mapped into a Markov chain model with a state space $S = \{S_i | 0 \leq i \leq n-1\}$, composed of n states. Meanwhile, a subset of this state space $A = \{S_j | 0 < j \leq n-1\} \subset S$ contains a number of states, which represent joining or connection of a node to the network, while the rest represent disconnection $A' = \{S - A\}$. In order to proceed, after the completion of Markov chain design, the values of the transition rates must be determined in form of the infinitesimal generator matrix $[Q]_{n\times n}$. In this regard, an extensive set of simulations must be conducted based on the sample frequency-based estimator technique to obtain $[Q]_{n\times n}$. Based on this approach, to obtain a precise

estimate of the generator matrix, a dense network scenario contained of M mobile nodes $MN_k, k \in \{1, 2, ..., M\}$ must be considered. In this network, every one of the nodes must accomplish their path selection based on the intended routing mechanism. Along with simulating the system for a long period of time (T), an enormous number of samplings (H) will be taken from the system in short periods of time (every (ΔI)). In the τ^{th} iteration of the sampling (ΔI_τ), where $\tau \in \{1, 2, ..., H\}$, and $T = \sum_{\tau=1}^{H} \Delta I_\tau$, every node will be monitored, and the state, where the node is located, will be logged as $S_i^{MN_k}(\Delta I_\tau)$. Consequently, with considering the residing states of node MN_k in two consecutive iterations ($S_i^{MN_k}(\Delta I_{\tau-1})$, and $S_j^{MN_k}(\Delta I_\tau)$), the number of transitions from S_i to S_j (represented with $N_{s_i \to s_j}^{MN_k}$) will be monotonically increased for this node. In addition, the number of transitions starting from state S_i ($N_{s_i}^{MN_k}$) will be also incremented by one unit. With completion of the simulation, according to Equation (3) in section II.B, the rate of transition between S_i to S_j will be calculated for node MN_k, and it will be represented as $(\lambda_{i,j}^{MN_k})$.

The aforementioned process should be accomplished simultaneously for all of the mobile nodes through the simulation period (T). Finally, based on the calculated values, the infinitesimal generator matrix will be obtained based on the following mathematical statement.

$$[Q]_{n\times n} = \frac{1}{M} \times \sum_{k=1}^{M} \begin{bmatrix} \lambda_{0,0}^{MN_k} & \lambda_{0,1}^{MN_k} & \cdots & \lambda_{0,n-1}^{MN_k} \\ \lambda_{1,0}^{MN_k} & \lambda_{1,1}^{MN_k} & \cdots & \lambda_{1,n-1}^{MN_k} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n-1,0}^{MN_k} & \lambda_{n-1,1}^{MN_k} & \cdots & \lambda_{n-1,n-1}^{MN_k} \end{bmatrix}$$

According to what we have discussed in section II.B, after obtaining the infinitesimal generator matrix Q, (8) will be used to determine a set of time-dependent differential equations for the states of the Markov chain.

$$\begin{bmatrix} P'_{S_0}(t) \\ P'_{S_1}(t) \\ \vdots \\ P'_{S_n-1}(t) \end{bmatrix} = [Q]_{n\times n} \times \begin{bmatrix} P_{S_0}(t) \\ P_{S_1}(t) \\ \vdots \\ P_{S_n-1}(t) \end{bmatrix}_{n\times 1} \quad (8)$$

Every one of the differential equations (corresponding to s_i), could be represented in form of the following:

$$\frac{dP_{S_0}(t)}{dt} = D_{S_0}(t), ..., \frac{dP_{S_{n-1}}(t)}{dt} = D_{S_{n-1}}(t)$$

These differential equations $(D_{S_i}(t))$, are then transformed into an algebraic equation via the Laplace transformation according to (9).

$$P_{S_i}(s) = \mathcal{L}(D_{S_i}(t))(s) = \int_0^\infty D_{S_i}(t)e^{-st}dt, S_i \in S \quad (9)$$

After solving the obtained equations, and using the inverse Laplace transform, the time-dependent equations of $P_{S_0}(t), P_{S_1}(t), ..., P_{S_{n-1}}(t)$ will be achieved. Finally, with considering all of the existing states in set A, the attachability of the routing protocol will be calculated and plotted based on (10).

$$A_T(t) = \sum P_{S_j}(t), \forall S_j \in \{A\} \quad (10)$$

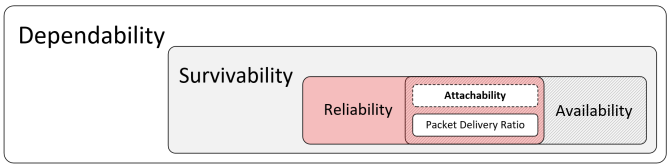


Figure 4: Relationship between different concepts.

Concept	Definition
Dependability	A wide context indicating the level of provided Quality of Service by the system during its life-cycle in a trustworthy manner.
Survivability	The ability of a system to serve in a timely manner in the presence of faults, errors, failures, threats, or accidents.
Availability	Probability of operating correctly, and being available for performing the specified tasks at every instance of time.
Reliability	Probability of operating correctly in a specific time interval, with the condition that the system was operating correctly at the beginning of that interval.
Attachability	The conditional probability that indicates the ability of a routing protocol in providing a successful connection to the network for the mobile and stationary devices at a certain instance of time, and maintaining their connectivity during a specified time interval.

Figure 5: Definition of different concepts.

Since the generator matrix reflects the communication alterations in the network, attachability could be considered as a sensitive metric, which could react to different communication-related factors in the network. From routing point of view, the parent selection policy, routing metrics, neighbor table placement, and replacement policies, and update rates of the routing tables are among the most important factors. On the other hand, there exist a number of sidelong parameters that are also effective. One of these factors is the movement pattern of the nodes, which is determined based on a specific mobility model [4]. The movement pattern of the nodes impacts on how the routing mechanism manages the disconnection of the nodes via handover procedures. Therefore, mobility models could also contribute to the amount of attachability. The area size, number of the nodes, and the transmission range of the radio modules are also effective. In this regard, in order to have a precise estimation of the generator matrix (corresponding to the pure path selection policies of the intended routing mechanism), and remove any other side-effects, the simulation scenario should be considered with significant care to remove any influential factors on the calculated attachability.

Based on its definition, attachability plays an important role in the entire reliability of a routing mechanism. Therefore, as it has been illustrated in Fig. 4, PDR, and attachability are both considered as the main building blocks of reliability in a wireless network. On the other hand, the reliability itself is part of survivability, and dependability, respectively. Hence, based on this hierarchy, attachability could be also used as an appropriate metric for evaluating the survivability, and dependability in wireless applications. Due to the tight relation between these concepts, it is important to have a clear view on their exact definitions to remove any uncertainties. Accordingly, Fig. 5 represents a brief description of these expressions.

A. Attachability Threshold (δ_a)

According to Fig. 3, there exists an attachability threshold (δ_a), which should be defined by the intended IoT and WSN applications. In this regard, the employed routing mechanism must comply with the specified level of threshold by the application. The process of specifying δ_a is similar to determination of threshold in reliability. Hence, in this section, we explain how the threshold value is determined for reliability, and then we conclude that the same approach could be applied for attachability. Let $\mathbb{T}$ be a non-negative random variable representing the life-time of an IoT device. Typically, the reliability of a device, or a system is given in terms of probability distributions that model the random variable $\mathbb{T}$. Meanwhile, the Weibull distribution with two parameters, $\mathbb{T} \approx W[\eta, \beta]$, is one of the most widely used models, due to its flexibility in characterizing Time-to-Failure *(TTF)* of devices with non-constant failure rates [61]. Weibull is a versatile distribution, which could take on the characteristics of other types of distributions, based on the value of its shape parameter β. The Weibull Reliability equation for the 3-parameter Weibull Cumulative Density Function *(CDF)* is given by (11).

$$R(t) = e^{-(\frac{t-\gamma}{\eta})^{\beta}} \tag{11}$$

Where η is the scale parameter (also known as life characteristic), β is the shape parameter (or slope), and γ is the location parameter (or the failure-free life). Value of γ represents the period, where no faults or errors occur in the intended device. Typically, the location parameter (γ) is considered as zero. Furthermore, different values of β can have significant effects on the behavior of the distribution. In fact, some values of β will cause the Weibull distribution equations to reduce to other types of distributions. For instance, when $\beta = 1$, the PDF of the 3-parameter Weibull distribution reduces to that of the 2-parameter exponential distribution. On the other hand, the Weibull failure rate function, $\lambda(t)$, is given by (12).

$$\lambda(t) = \frac{\beta}{\eta}(\frac{t-\gamma}{\eta})^{\beta-1} \tag{12}$$

In case $\beta = 1$, we will have $1/\eta = \lambda$, where λ is an indication for the failure rate. Accordingly, if we assume $\gamma = 0$, the Weibull reliability, and failure rate functions could be rewritten as in (13), and (14), respectively.

$$R(t) = e^{-(\frac{t-\gamma}{\eta})^{\beta}} = e^{-(\frac{t-0}{\eta})^{1}} = e^{-\lambda t} \tag{13}$$

$$\lambda(t) = \frac{\beta}{\eta}(\frac{t-\gamma}{\eta})^{\beta-1} = \frac{1}{\eta}(\frac{t-0}{\eta})^{1-1} = \frac{1}{\eta} = \lambda \tag{14}$$

As mentioned earlier, manufacturers of devices are responsible for determining the threshold value for the reliability of their products [62]. The most widely used measure for this threshold is the Mean-Time-to-Failure *(MTTF)*, which indicates the average life of a device, or the time interval when approximately 50% of the produced devices will fail. The MTTF of the Weibull PDF is calculated by (15).

$$MTTF = \gamma + \eta.\left[\Gamma(\frac{1}{\beta}+1)\right] \tag{15}$$

Where $\Gamma(x)$ is the Gamma function evaluated for x. It is worthy to mention that the Gamma function for an integer parameter $n > 0$ is defined as in (16).

$$\Gamma(n) = \int_0^{+\infty} e^{-x}x^{n-1}\,dx = (n-1)! \tag{16}$$

With considering our primary assumptions, $\gamma = 0$, and $\beta = 1$, the amount of MTTF could be derived from (17).

$$MTTF = 0 + \eta.\left[\Gamma(\frac{1}{1}+1)\right] = \frac{1}{\lambda} \tag{17}$$

As it has been indicated in equation (17), MTTF and the rate of failure could be derived from one another. Hence, in order to obtain the reliability threshold, manufactures must first conduct a set of real-world experiments on their devices to obtain MTTF, and consequently λ. This could be achieved via determining the number of failures. The acceptable number of failures is the maximum number of failures allowed for the total number of devices considered during their average life. After determining the amount of MTTF, they will specify the reliability by means of λ, and provide it as a standard for that specific application. For instance, authors in [63] have indicated that a reliable fire detection wireless sensor network equipped with mini photo-voltaic cells *(PV-WSN)*, has a MTTF $>$ 60 days. After the production, the manufacturer, and researchers will try to meet this threshold through proposing new techniques. The proposed approach must undergo redesign exercises in case that the aftermath tests show that this target has not been achieved.

The same approach could be applied to attachability. The only difference would be that instead of MTTF, we need to define a new parameter such as Mean-Time-to-Disconnection *(MTTD)*. Similar to MTTF, the value of MTTD should be also measured via real-world wireless applications to obtain the average time period, where a node gets permanently disconnected from the network. Based on the obtained value, a standard value for attachability could be determined and scholars and designers can consider that value as their target threshold when proposing new communicating technologies.

With understanding the concept of attachability, and its calculation, in the following sections, attachability has been described, and evaluated in detail for the RPL routing protocol. This protocol has been selected, because it is broadly used in IoT infrastructures.

V. Description of Attachability for RPL

The movement status of the nodes could be generally classified into two modes: 1) Moving, and 2) Not-Moving. In case that the nodes have dynamic movements, they will traverse the area based on a specific mobility pattern, otherwise they will have a stationary behavior without changing their location. Based on the attributes of attachability, different parts of RPL could directly affect the pre-junction, and post-junction functionalities and consequently alter the value of attachability. Therefore, the employed objective function, routing metrics, path selection policies, neighbor table replacement policies, control packet structure, and their dissemination, and also the trickle algorithm could significantly impact the amount

of attachability in RPL. Meanwhile, the control packet dissemination mechanism has a pivotal role. In the pre-junction phase of this protocol, the DIO and DIS messages will be the main players, while during the post-junction, the DIO and DAO messages will be the dominating factors for maintaining the level of attachability. In the following, the key effective operations in the overall attachability of RPL will be addressed in each of the mentioned phases.

A. Pre-Junction Phase

In the pre-junction phase, upon boot-up, a soliciting node can decide to stay silent and keep listening to the radio channel for probable incoming DIO messages containing the required information for joining a DODAG, or it may decide to send DIS messages for probing nearby DODAG members. In case of deciding to send DIS messages, the node waits for DIOs containing routing information such as metrics, routing costs, Mode of Operation *(MoP)*, and DODAG affiliation. When a new-coming node tries to join a DODAG, independent from its movement, there is a probability that its DIS messages may not be successfully delivered to its neighboring nodes. While the existing factors in the harsh wireless IoT environments, e.g., thermal noise, scattering, and reflection are believed as the dominating factors for the signal disruption and prevention for a successful delivery of the packets to the destinations, there are few other issues that could severely affect the delivery of the packets in the network. In particular, the packet loss in an IoT node could be due to its high speed movement (in case of having mobility), which prevents it from establishing a successful connection, or in case that there exists no other nodes in its transmission range. In such cases, the node would not be able to successfully deliver its DIS packets. Hence, it would be impossible for the node to join the DODAG and attach to it.

Based on the structure of RPL, in case that the DIS message has been broadcasted successfully by the joining node, a subset of DODAG nodes, which have received that DIS, must send a unicast DIO message back to the DIS transmitter. It should be mentioned that RPL considers a local timer, which after its expiration, if the node does not receive any DIOs, it will start broadcasting DIO messages itself as a root of a floating DODAG until it joins a grounded DODAG [12]. In many cases, being a root of a floating DODAG is not desirable for those nodes, who are battery operated or energy harvested. Therefore, RPL also considers a timer for preventing the nodes to stay as a root of a floating DODAG for a long period of time. If the soliciting node receives the DIO, three items will be checked for evaluating whether the node can join the DODAG or not: 1) RPL Instance ID, 2) List of supported routing metrics and constraints, and 3) Specified objective function in the Objective Code Point *(OCP)*. Any node, who desires to be connected to a DODAG, must honor the specified MoP and objective function. Otherwise, the node will not be allowed to join as a router. In such situations, it will be only granted to join as a leaf, or in a number of scenarios specified by the policies of RPL, it will be rejected to join the DODAG. Furthermore, in case that the received DIO message is corrupted or it contains metrics or constraints that are not understandable or supported, the soliciting node will be only able to join as a leaf or even it will not be permitted to connect to the DODAG at all. Consequently, the probability of success in joining the DODAG, highly depends on whether the correct DIO messages have been successfully transmitted from the intended members of the DODAG, and also a successful receipt of at least one of them by the joining node.

In this regard, here are several factors that can contribute to an unsuccessful delivery of a DIO message. First, a DIO message can become corrupted due to different sources of noise, e.g., white Gaussian noise, interference, distortion, bit synchronization problems, attenuation, wireless multi-path fading, or other environmental disturbance factors. On the other hand, as it could be derived from (11), since the packet length (L) of the DIO messages are longer than the DIS messages, their error rate (PER) is typically higher than the DIS messages. Therefore, one of the existing approaches for enhancing the amount of attachability in the RPL routing protocol is to reduce the size of the control packets as small as possible (especially in relatively harsh environments with high amounts of Bit Error Rate (BER).

$$\begin{aligned} PER &= 1-(1-BER)^{L}, \\ L_{DIO} \geq 24Byte, L_{DIS} &\geq 2Byte \\ \Rightarrow PER_{DIO} &> PER_{DIS} \end{aligned} \tag{18}$$

Apart from the control packets, their dissemination mechanism, which is governed by the trickle timer also plays an important role in the overall attachability of the RPL routing protocol [20]. Accordingly, in RPL-based mobile IoT applications, if the predefined timing parameters for the trickle timer have been set to values that the interval between the transmission of two consecutive DIO messages would be too long, the DIO sender may leave the reception range of the joining node, before successfully delivering the DIO message. In contrast, by reducing the time interval, the DIO message will have the opportunity to be delivered to the joining node on time. Nevertheless, this will be obtained with a cost of more energy consumption by the nodes. Thus, there will be a trade-off between attachability and energy consumption in certain perspectives.

RPL supports message confidentiality, authenticity, and integrity. Therefore, it employs three modes of security: 1) Unsecured, 2) Pre-installed, and 3) Authenticated [12]. In the second, the nodes, who want to join the DODAG, have a pre-installed key, which enables them to generate and process secured RPL messages, and join the DODAG as either leaf or router. On the other hand, in the third mode, while the nodes still have the keys for joining as a leaf, but in case that they want to join as a router, they must obtain a second key from a key authority. Furthermore, the authentication-enable flag in the body of DIO plays an important role in allowing the nodes to join a DODAG. Occurrence of attacks or any issues regarding the considered security-related sections in DIO, DIS, and DAO messages could prevent a node to join the network successfully. The fault management mechanisms, which are considered in RPL, could also prevent the nodes from joining

the DODAG for the first time or rejoining at a later instance of time [12].

B. Post-Junction Phase

Once the node has successfully became a member of a DODAG, the RPL upward route discovery enables the nodes to discover the members of the intended DODAG and add them to their neighbor table list, and select them as their preferred parent. This is one of the most important tasks in the post-junction phase, which is managed by the specified policies in the objective function. Depending on different factors, RPL gives this option to the nodes to join another DODAG within the RPL instance, while their current DODAG is still honoring the optimization objectives. Occurrence of any issues during this transition may lead into disconnection. For instance, if the node was previously a member of the targeted DODAG, RPL will not allow the node to rejoin it with advertising higher rank values than the specified value. While this action is helpful for preventing loophole, resource wasting, and also providing security measures, it may lead into connection failures.

In case that a node becomes disconnected from its parent, the three following scenarios are possible:

1) The current (disconnected) parent was the only candidate parent in the node's neighbor table: In this case, since there are no other alternatives, the node will leave the DODAG.
2) More than one candidate parents exist in the neighbor table: Based on the objective function, a new substitute parent will be selected from the neighbor set.
3) The neighbor set was full: The current (disconnected) parent will be replaced with a new parent selected from the neighbor table, and it will be removed from the table to open up free entry for probable new neighbors. However, if the connection is still active, and the parent switch was only conducted due to quality degradation of the link, the node will not be removed from the neighbor table; unless the RPL detects that a new neighbor could provide a better connection, which in this case, the parent will be replaced with the new candidate.

When a non-root node faces with an empty neighbor table, RPL triggers a local timer for that node before preventing it from being associated with the DODAG anymore. In mobile networks, this timer turns into a vital element; because, the nodes could frequently encounter an empty neighbor table due to their dynamicity. In contrast, when the node's neighbor table becomes fully occupied, the replacement policies become important for maintaining the most appropriate candidates in the table [3]; this highly depends on the size of the neighbor table defined by RPL and also hardware specifications of the deployed nodes in the area. Generally speaking, while a node is a member of a DODAG, connection failures could occur due to different reasons. First, the node might not receive any DIO messages from its parent for a long period of time due to the previously mentioned factors. Moreover, the node might send a DAO message and do not receive the DAO-ack from its parent. In this case, the probability of disconnection depends on the number of times the node has tried to send a DAO to its parent and did not receive any acknowledgments. For instance, if the node has sent five DAO messages to its parent but has not received any DAO-acks, it could be assumed that the connection has been permanently terminated.

As part of the fault management mechanisms defined in the structure of RPL, to provide more stable connections, nodes may be disconnected from their DODAG, even if their optimization objectives determined by the objective function are still honored. Accordingly, the two of the most important cases are:

1) Global repair: Which is declared by the root, and all of the nodes that were members of the intended DODAG will be enforced to get disconnected, and must try to rejoin the new constructed DODAG.
2) Local repair: Due to occurrence of inconsistencies in a specific area, e.g., loops, the node itself will terminate its connection, and try to rejoin the same DODAG.

Each time the root declares a global repair, the value of the DODAG version number will be monotonically increased by the root. In this case, if any node does not successfully update its stored version number, it will be banned from acting as a parent, which could turn into a serious problem for those nodes, who want to connect to the DODAG via that specific node. It should be also mentioned that a global repair does not affect a node, which is not yet a member of a DODAG. One of the approaches taken by the RPL to prevent loops in the DODAG, and remove the necessity of local repairs, is to not allow the nodes to have a greedy behaviour. A node is called greedy, when it tries to connect to the high-ranked nodes in the bottom of the DODAG. After joining the network, based on the employed rank calculation mechanism, RPL does not allow the new node to act as a greedy node, which may lead into permanent ban of that specific node from joining the network.

C. Markov Chain Model of the nodes connectivity in RPL

Based on all of the actions taken by the RPL protocol during the pre-junction, and post-junction phases for establishing, and maintaining the connection of the nodes, the status of the node's connection to the DODAG has been mapped into a Markov chain model, and has been depicted in Fig. 6. This figure represents the transitions between the states from an IoT node point of view. This model covers all of the possible states that a mobile node could reside based on the RPL RFC 6550 [12]. The 33 states of this Markov chain model could be mainly distinguished from the following perspectives: 1) Status of the movement (mobile or stationary), 2) DODAG membership (connected or temporary disconnected), 3) Status of the parent table (number of available candidates), and 4) Permanent disconnection. In this state diagram, it has been assumed that all of the nodes start from the stationary state S_0, where the node is not connected to the DODAG. As long as the node is stationary and it is not able to join the DODAG, it will reside in this state. On the other hand, while the node is still stationary, but it inserts a candidate parent to its neighbor table, and joins the DODAG, it will make a transition from S_0 to S_3. In addition, whenever the node starts moving, based

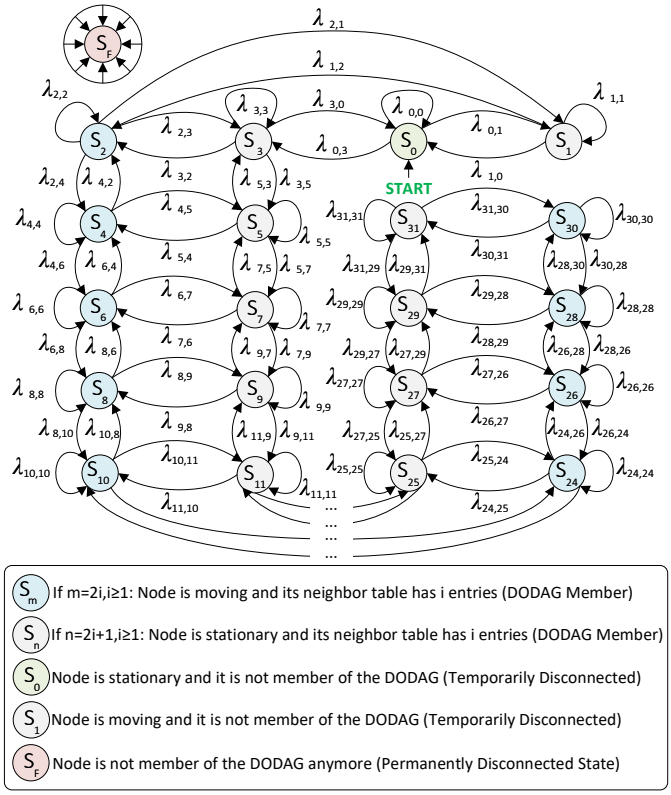


Figure 6: The Markov chain model of attachability in RPL.

on whether it has not been able to join the DODAG, or it has been able to join the DODAG by adding a candidate parent to its neighbor table, and selecting it as its parent, it could make a transition from S_0 to S_1 or S_2, respectively.

According to RFC 6550, RPL considers 15 entries for the neighbor tables of the nodes. Therefore, the number of candidate parents in a table could vary between 0 (empty) and 15 (fully occupied). The number of existing candidates in the neighbor tables could be an indication for the status of connectivity of a node. For instance, a node with one candidate parent has a fragile connectivity to the DODAG, because with losing that parent it will get disconnected from the DODAG. On the other hand, a node with five candidates in its table has a more robust connectivity, as if it loses one candidate, it has four remaining options to replace the lost parent. Therefore, based on inserting a candidate parent to the table, nodes can make a transition from S_{i-1} to S_i ($i \geq 1$ is the number of candidate parents in the neighbor table), and in case they lose any parents based on the policies of RPL, they will make a transition from S_i to S_{i-1}. Furthermore, it is important to know the movement status of the nodes as the mobility-aware versions of RPL differentiate between mobility and stationary states. Accordingly, based on the 15 entries of the tables, in case that a node has at least one candidate parent in its table (which is considered as connection to the DODAG), there will be $2 \times 15 = 30$ states for both mobile and stationary states (S_m, and S_n states in Fig. 6). Two states, including S_0, and S_1, represent temporary disconnection to the DODAG (indicating no candidates in the neighbor table) in stationary, and mobile conditions, respectively. Finally, in any point of time, and in any states, there is a possibility to move to the permanent disconnected state S_F due to disabilities of the routing mechanism in keeping the connection to the DODAG.

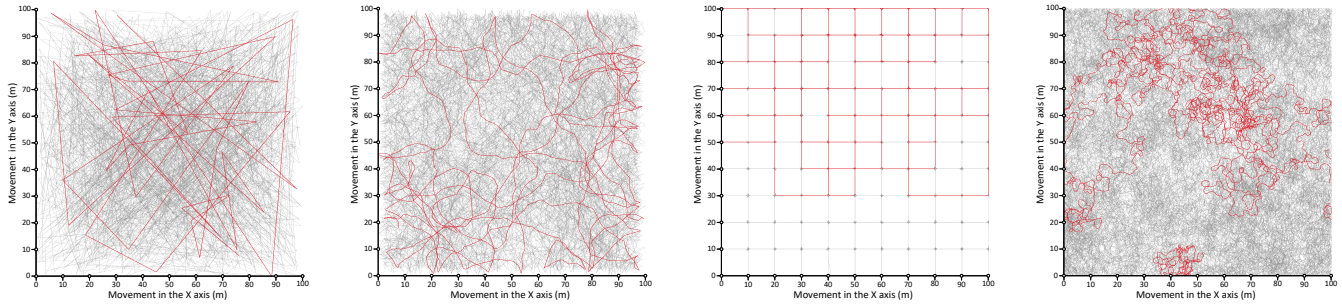
Regarding the status of movement, it should be noted that in mobile applications, nodes could be permanently fixed, e.g. the side-road units in VANETs, or they could have movement with no or partial stops (known as pause) through their trajectory. The movement behavior of the nodes such as pause times, velocity, distance between the stopping points, individual or group movements, selection of destinations, obstacles, impediments, and the existing restrictions in the motion are all dependent on the mobility pattern of the nodes [4]. According to Fig. 6, whether the nodes are continuously moving or spending their pause times before starting another trip, they will be resided in the moving states (S_1 or S_m). In case they pause for a period longer than the maximum amount of allowed pause time in the intended mobility model, it will be assumed that they have made a transition to a stationary state (S_0 or S_n). As soon as they get displaced (considering their coordination), they will make a transition to a moving state again. Otherwise, they will stay in the stationary state.

Based on the above mentioned issues, the pre-junction and post-junction tasks in the structure of a routing mechanism, and consequently the connection and disconnection of the nodes to the DODAG could mainly represent themselves in form of insertion or remove of parents in the neighbor tables. Therefore, there is an implicit correspondence between the pre-junction and post-junction tasks and the states of Fig. 6. As a result, with any modifications to these tasks, the capability of routing in managing the connections will alter, which affects the transitions from one state to another. As it was discussed, independent from the movement status of the nodes, an empty neighbor table does not necessarily indicate the permanent disconnection from the DODAG, and based on the RPL structure, the nodes will be given an opportunity to try to connect to the same or another DODAG within the RPL instance again. Therefore, in any circumstances that the node is not able to connect to the DODAG again, it will be assumed as a permanent disconnected node, and it will reside in sate S_F, where the attachability is considered as 0.

As part of the attachability calculation road-map (Fig. 3), in the next section, the conducted experiments for obtaining the infinitesimal generator matrix, and consequently the calculation of $A(t)$ will be described in detail.

VI. System Setup and Case Study Evaluations

For conducting our evaluations, a 10000m^2 sensing area has been considered in the Cooja simulation environment. Cooja is a cycle-accurate Java-based simulator, which is implemented as part of the Contiki operating system [18], [64]. This open-source tool is able to simulate/emulate well-known IoT platforms in different levels of abstraction. According to Table. I, based on the intended simulation scenario, the area is composed of different number of nodes indicating various sensing densities. In every scenario, 20% of the nodes are devoted to anchors representing fixed-place nodes, while the



(a) Random Way-Point (b) Gauss-Markov (c) Manhattan (d) Boundless Area

Figure 7: Trajectory of the Nodes Under the Presence of Different Mobility Models.

Table I: Simulation environment parameters.

Parameter	Description
Sensing Area	10000m^2
Number of Transmitter Nodes	15, 25, 35, 45
Number of Mobile Nodes	80% of Transmitter Nodes
Number of Anchor Nodes	20% of Transmitter Nodes
Number of Sink Nodes	1
Communication Range	20m
Interference Range	30m
Transmission Power	0dBm
Transmission Interval (TI)	60 Seconds
UDP Payload Size	48 Bytes
Simulation Time	12 Hours

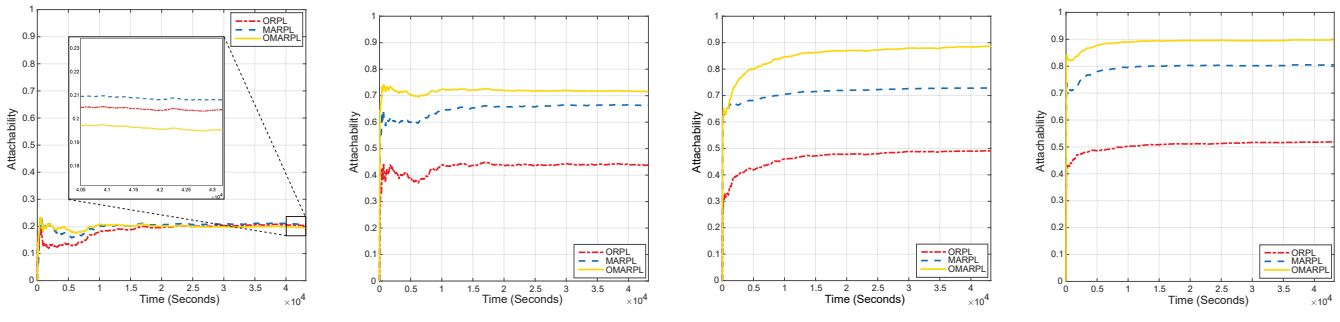
Table II: Zolertia One specifications.

Parameter	Description
Micro-Controller Unit (MCU)	MSP430 (2nd generation)
Architecture	16 bit RISC (Upgraded to 20 bits)
Radio Module	CC2420
Operating MCU Voltage Range	1.8V$<V<$3.6V
CC2420 Voltage Range	2.1V$<V<$3.6V
Operating Temperature	-40°$C<\theta<$+85°C
Operating System Clock Frequency	$f<$16MHz
MCU Active Mode Current @ V_{cc} = 3V (I_a)	2mA
MCU Low Power (Standby) Mode Current (I_{lpm})	0.5 μA
Off Mode Current	0.1 μA
Radio Transmitting Mode Current @ 0dBm (I_{tr})	17.4mA
Radio Receiving Mode Current (I_{rc})	18.8mA
Radio IDLE Mode Current	426 μA

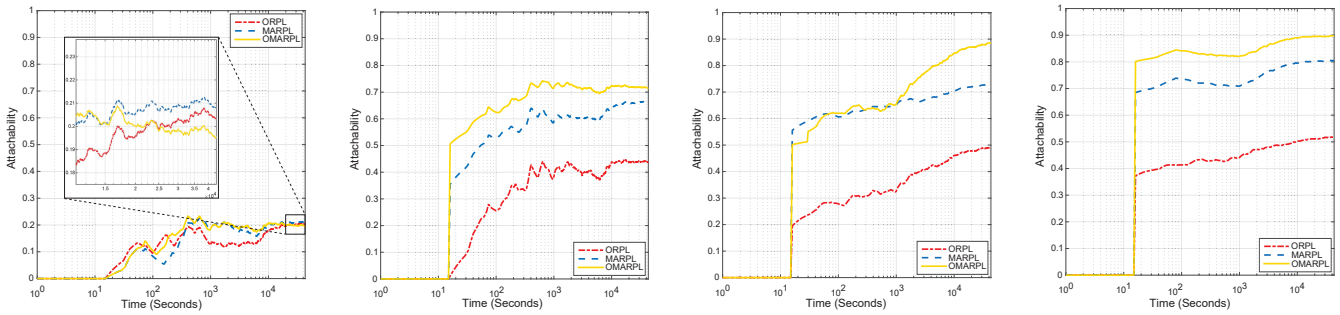
rest are moving based on the exploited mobility model. The RPL instance is contained of only a single sink, obliged to control the DODAG, and collect the transmitted packets from the network. The nodes are set to transmit UDP packets with a 60 second transmission interval.

The deployed nodes in our simulation environment are a group of COTS IoT platforms, known as Zolertia® One (Z1), which employ the well-known Texas Instruments® low-power MSP430 micro-controller, and the Chipcon® CC2420 radio transceiver. The major hardware specifications of Z1 and its interior modules are extracted from their data-sheet and illustrated in Table II. In our simulations, the nodes are set to send their packets with a transmission power of 0dBm, as it has been considered as the default value in many real-world WSN and IoT applications [65]. Furthermore, according to Table. I, the transmission and interference ranges of the Z1 nodes are set to 20 and 30 meters, respectively. Finally, as it was mentioned earlier, as part of the sample frequency-based estimating technique, in order to reach precise attachability values in the steady state, all of the simulations were lasted for 12 Hours, considering the network's convergence time. The movement pattern of the nodes in the area has a direct impact on the performance of the routing policy and how it responds to the frequent connections and disconnections of the mobile nodes from their attachment point [4]. Therefore, as part of our comprehensive evaluations, we have considered four different types of mobility models in order to analyze the effect of mobility models on the attachability of the routing policies. These models include: 1) Random Way-Point (RWP) [66], 2) Gauss-Markov (GMM) [67], 3) Manhattan (MMM) [68], and 4) Boundless-Area (BSA) [19]. Furthermore, in order to be able to fairly justify the outcome of the simulations, we have simulated and illustrated the trajectory of the nodes under the presence of each mobility model in Fig. 7. The interested reader could get more details about the structure of these mobility models in [4]. Finally, in order to evaluate the pivotal impact of different routing policies on the attachability, we have considered three different versions of RPL in our simulations, including the original version of RPL (ORPL) [12], and two mobility-aware extensions of this protocol, known as MARPL [16], and REFER (also called OMARPL) [17].

With considering the RWP mobility model, the amount of provided attachability by ORPL, MARPL, and OMARPL has been depicted in Fig. 8. As it could be observed, independent from the routing policy, with increasing the number of deployed nodes in the area (higher node density), the amount of attachability will be enhanced. To get into more detail, consider a soliciting node, which seeks to join or rejoin a DODAG. Assume that the node may face two different scenarios: 1) Existence of 10 surrounding neighbor nodes, and 2) Existence of only a single nearby node. Accordingly, in the first case, there will be a higher probability of successfully receiving at least one DIO message by the soliciting node compared to the second scenario. Therefore, with deploying more number of nodes in the area, the amount of attachability will be significantly improved. As it has been depicted in Figure. 8, the average amount of attachability in the 45 node scenario has been increased by up to 73% compared with the 15 node scenario. This is the reason that we have previously emphasised that the sidelong factors, such as the number of the nodes, must be carefully selected to remove any side-effects on the calculation of attachability. It should be also mentioned that in case of low-density networks, e.g., Fig. 8: (a), due to lack of path diversity in the DODAG, all of the

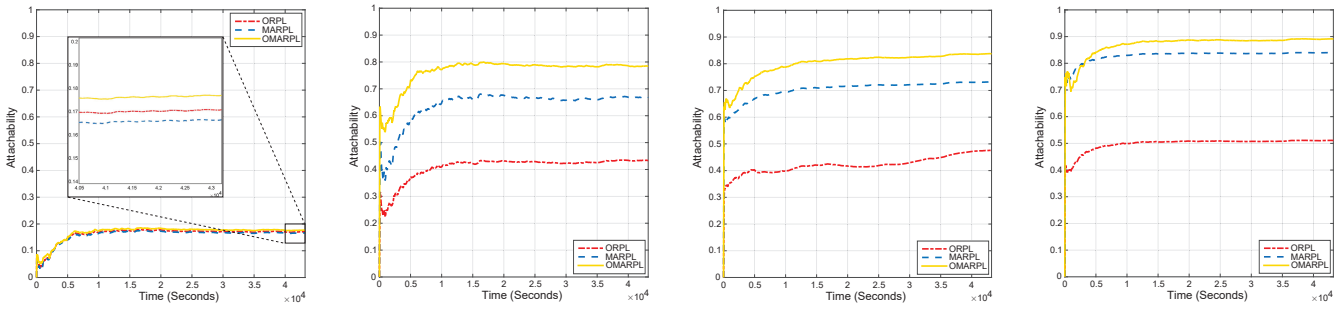


(a) 15 Node Scenario: Linear Scale (b) 25 Node Scenario: Linear Scale (c) 35 Node Scenario: Linear Scale (d) 45 Node Scenario: Linear Scale

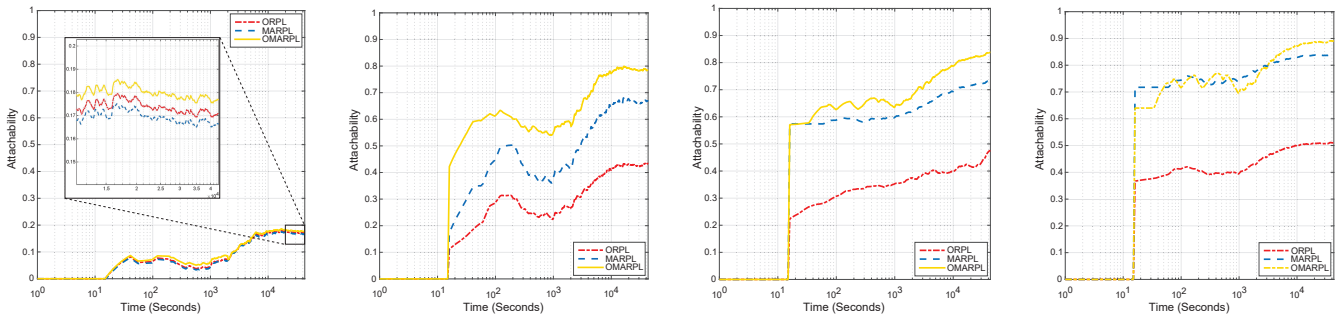


(e) 15 Node Scenario: Log Scale (f) 25 Node Scenario: Log Scale (g) 35 Node Scenario: Log Scale (h) 45 Node Scenario: Log Scale

Figure 8: Evaluation of Attachability for ORPL, MARPL, and OMARPL in Presence of Random Way-Point Model (RWP).



(a) 15 Node Scenario: Linear Scale (b) 25 Node Scenario: Linear Scale (c) 35 Node Scenario: Linear Scale (d) 45 Node Scenario: Linear Scale

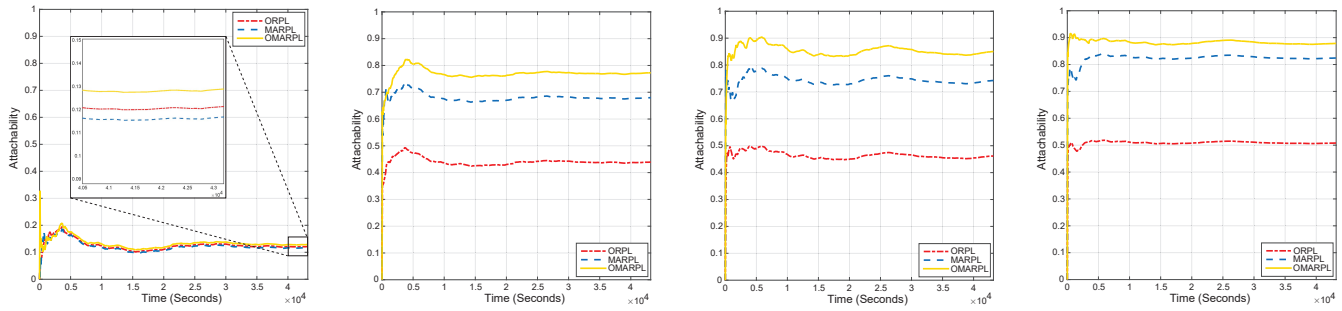


(e) 15 Node Scenario: Log Scale (f) 25 Node Scenario: Log Scale (g) 35 Node Scenario: Log Scale (h) 45 Node Scenario: Log Scale

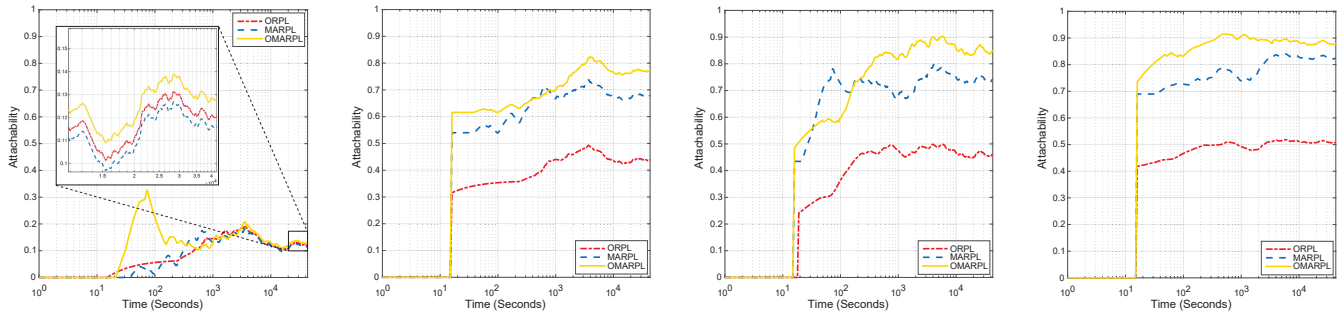
Figure 9: Evaluation of Attachability for ORPL, MARPL, and OMARPL in Presence of Gauss-Markov Mobility Model (GMM).

routing policies are acting relatively the same. Because, due to the presence of limited number of nodes in the transmission range of the mobile nodes, the neighbor table of the nodes will be composed of only a single or few candidates. In such cases, the nodes may have no other option but to select the available candidate as their preferred parent without considering the routing policy. Therefore, different OFs would not be able to get fully effective and they show the same amount of attachability.

In addition to the linear scale representation of the graphs, in order to provide a more clear picture of the attachability alterations through the time in all of our simulations, the

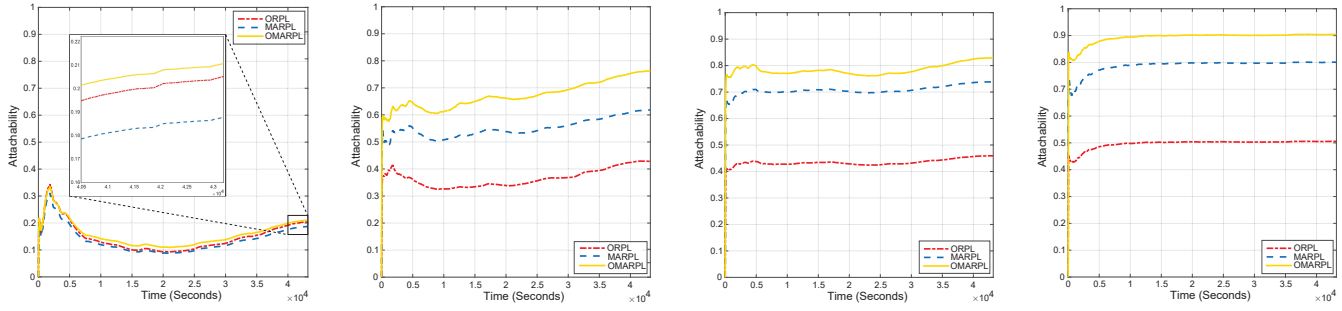


(a) 15 Node Scenario: Linear Scale (b) 25 Node Scenario: Linear Scale (c) 35 Node Scenario: Linear Scale (d) 45 Node Scenario: Linear Scale

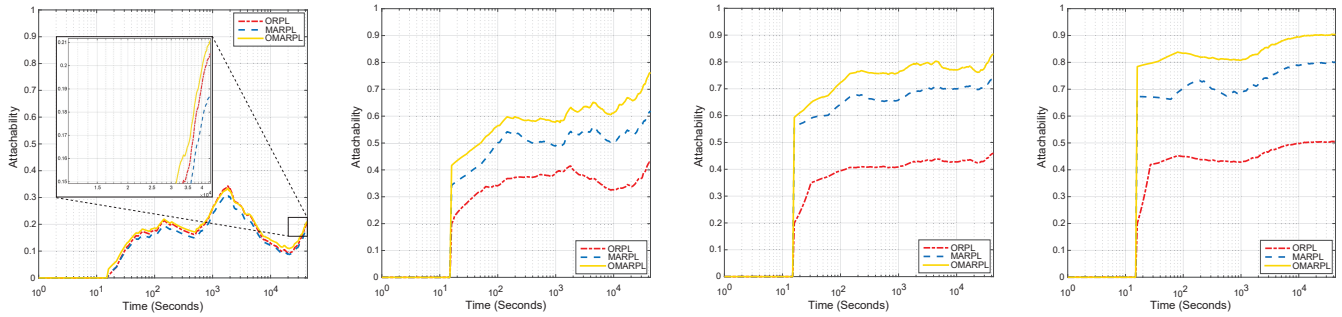


(e) 15 Node Scenario: Log Scale (f) 25 Node Scenario: Log Scale (g) 35 Node Scenario: Log Scale (h) 45 Node Scenario: Log Scale

Figure 10: Evaluation of Attachability for ORPL, MARPL, and OMARPL in Presence of the Manhattan Mobility Model (MMM).



(a) 15 Node Scenario: Linear Scale (b) 25 Node Scenario: Linear Scale (c) 35 Node Scenario: Linear Scale (d) 45 Node Scenario: Linear Scale



(e) 15 Node Scenario: Log Scale (f) 25 Node Scenario: Log Scale (g) 35 Node Scenario: Log Scale (h) 45 Node Scenario: Log Scale

Figure 11: Evaluation of Attachability for ORPL, MARPL, and OMARPL in Presence of the Boundless Mobility Model (BSA).

results have been also plotted in the logarithmic scale (Fig. 8: (e)-(h)). As it could be observed, at the beginning of the DODAG creation, the attachability is relatively low; because only a few nodes have joined the DODAG, and started their communications. As the time passes, and we move towards the steady-state, more number of mobile nodes will join the DODAG, which results in more pervasive communications and consequently higher attachability. Accordingly, in addition to employing higher number of nodes in the area, it is significantly important to report the provided attachability of

a routing policy, when the DODAG reaches its steady-state (end of the simulation time-line). Because in the middle of the simulations, or in cases, where the simulation period has been set to a short value, all of the mobile nodes will not have the opportunity to join the DODAG, and the network would not be completely created. Hence, due to lack of path diversity, the multi-hop feature will be eliminated from the network, and different routing policies will not be able to show their true path selection distinctions, which is the key effective factor on their attachability. According to Fig. 8, in case of having RWP as the mobility model, the amount of provided attachability by the original version of RPL (ORPL) could reach as high as 52%, while in case of having MARPL, and OMARPL, its value could reach as high as 81%, and 90%, respectively.

The reason behind the improvement of attachability in MARPL, and OMARPL against ORPL is the exploitation of mobility-based metrics, adjustment of the trickle algorithm, and also employment of mobility-aware neighbor table replacement policies, which enables them to better adjust with the movement of the nodes in the DODAG. Meanwhile, according to Fig. 8, in case of having the RWP mobility model, OMAPRL has improved the amount of attachability with an average value of 10% compared with MARPL, while this amount of improvement could reach as high as 17% based on the network density. The main reason for such an improvement relies beneath the path selection policy in OMARPL. According to [17], due to utilizing a novel neighbor table replacement policy in OMARPL, every entry in the neighbor table has been assigned with a leasing time, which unlike the MARPL, enforces the mobile nodes to frequently check the tables for purging the disconnected candidate parents, and bring up free space for detecting and inserting high-quality nearby candidate parents. In addition, since the selection of stationary nodes as the preferred parent has a higher priority than the mobile nodes, the general stability provided by the OMARPL is higher than MARPL [17]. All of the mentioned issues justify the better attachability provided by the OMARPL against MARPL.

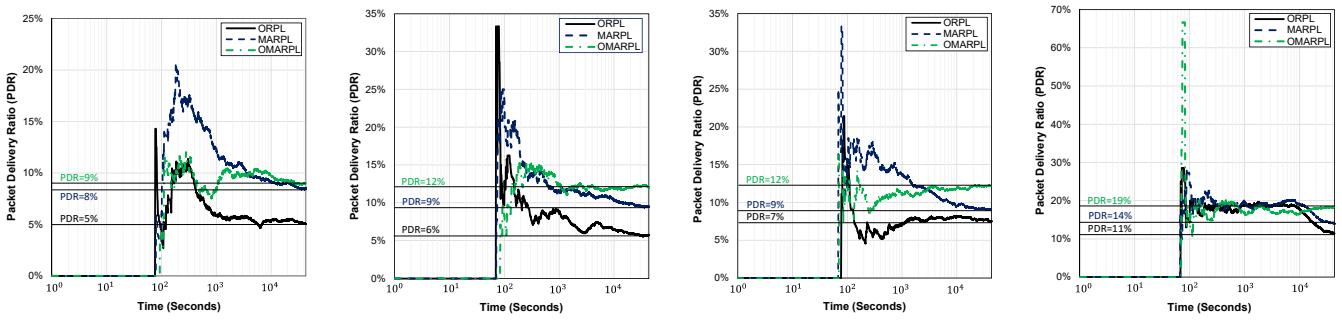
All of the mentioned justifications could be also extended to other mobility models. As it has been depicted in Fig. 9, Fig. 10, and Fig. 11, in case of using any other mobility models for the movement of the nodes, ORPL shows the minimum amount of attachability, while the two other mobility-aware versions of RPL have significantly improved the attachability. Similarly, OMARPL has provided better attachability compared with MARPL. On the other hand, with comparing the results in all of theses figures, it could be observed that the performance of the routing policy in terms of attachability, also depends on the type of the nodes movement pattern. For instance, with considering the OMARPL as our underlying routing policy in the 45 node scenario, with 86%, the MMM has lead into the lowest amount of routing attachability, while the BSA has resulted the highest value with 91%. The main reason relies beneath the structure of the nodes movement in these models. For instance, based on the movement structure of the nodes in MMM, due to the uniform distribution of the nodes on the grid, along with the geographical restrictions, which enforces the mobile nodes to move in horizontal and vertical streets (Fig. 7(c)), nodes are faced with lower number of available options as their candidate parents in their neighbor table list [4]. Therefore, as it is expected, the amount of attachability has been decreased compared with BSA, RWP, and GMM models. On the other hand, due to the closed torus-shaped simulation surface of the BSA, the nodes have a smooth movement without having any long straight flights (Fig. 7(d)). In addition, the nodes move around the same region for a long time, which enables them to remain connected to the same parent for a long period of time without requiring to switch to a new attaching point [4]. Accordingly, it is also important to consider the type of the movement pattern while calculating the attachability of a routing policy.

A. Attachability and Packet Delivery Ratio (PDR)

In this section, the more elegant role of attachability against PDR in determining the overall reliability of a routing mechanism is discussed. Our goal here is to show that reporting the reliability in terms of PDR will not specify the main cause for a better or weaker routing policy than the other one. More specifically, in addition to low attachability, there are few other factors affecting the overall reliability of a routing mechanism, e.g., congestion, and collision. When talking about PDR, it is not clear why the routing mechanism has provided a certain level of reliability. In other words, PDR is an opaque high-level metric for reliability, while attachability is one of the key low-level contributing factors affecting the overall reliability. Considering the 45 node scenario, the amount of provided PDR by different routing protocols is depicted in Fig. 12.

Although this figure is plotted in a continuous-time manner to make a correspondence between attachability and PDR figures, unlike attachability, PDR is not reported as a function of time. As it could be found in all of the existing studies, PDR is measured at the end of the simulation period. In other words, based on the definition of PDR, it does not represent the fluctuations of packet deliveries during the operation of the network. For instance, according to Fig. 12, independent from the mobility model, you can see that in some points of time, PDR is ascending, while in some intervals it is descending. Traditionally, with neglecting all of these alterations, the final amount of PDR is reported after the entire simulation period for every routing mechanism. For instance, in case of using the Gauss-Markov mobility model, the average amount of PDR for ORPL, MARPL, and OMARPL is 6%, 9%, and 12%, respectively. In contrast, attachability could be reported at any point of time making it a better, more informative, and more precise metric.

According to the literature, PDR in a network is obtained by dividing the number of successfully received packets by the sink, to the total number of transmitted packets towards it by the existing nodes. With assuming a constant, or variable packet transmission rate for all of the nodes, as soon as connecting to the DODAG, and beginning packet transmission, every node initiates a counter for counting the total number of transmitted packets, leading into higher denominator in the above mentioned definition for PDR. This is the reason that even if the PDR was reported in sequential time slots (similar



(a) Random Way-Point Model (b) Gauss-Markov Mobility Model (c) Manhattan Mobility Model (d) Boundless Mobility Model

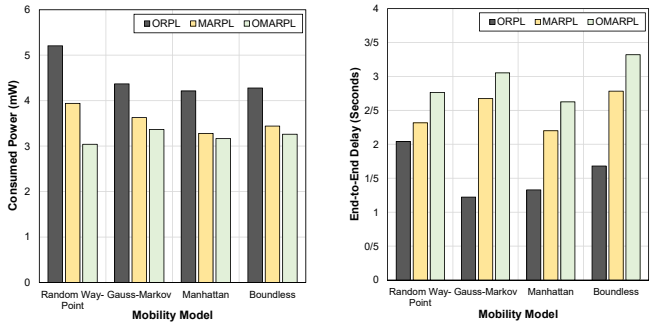
Figure 12: Evaluation of PDR for ORPL, MARPL, and OMARPL in Presence of Different Mobility Models (Log Scale).

to Fig. 12), it was not possible to report it in intervals shorter than the period between two consecutive packet transmissions. On the other hand, even with enhancement of attachability, which provides more connectivity in the network, and enables having higher PDR, other factors such as congestion could mitigate the amount of achievable improvement. Therefore, as the simulation passes the network's convergence time and moves towards the end of the simulation, the slope of increase in the number of successfully delivered packets will be equal or lower than the slope of increase in the total number of transmitted packets towards the sink. Accordingly, as it has been depicted in Fig. 12, in long-term analysis, PDR is a descending or constant function of time.

Generally speaking, with taking into consideration the results of attachability, and PDR, it could be concluded that in order to have a high PDR, and reliability, it is necessary to have a high attachability, but high attachability itself does not guarantee high PDR. It is possible to have a network with high amounts of attachability, but due to setting high transmission rates for the nodes, and limited transceiver buffers in the intermediate nodes, network becomes congested, and nodes have no other option but to drop the packets, leading into lower PDR [2]. Hence, in order to increase PDR and reliability in a wireless network, in addition to employing efficient flow-control techniques, the routing mechanism must also provide high attachability. Based on the results of simulations, among the three versions of RPL, OMARPL provided the highest amount of attachability, while it has also provided the highest amount of PDR in the network. On the other hand, ORPL showed the lowest amount of attachability, while it has provided the lowest PDR among the three versions. As a final note, it could be mentioned that PDR is a useful metric for comparing more than one routing mechanisms, while attachability could be used for evaluating the performance of a single or more number of routing mechanisms, especially in mobile IoT, and WSN applications. This metric is believed as one of the key factors in the overall reliability of a routing policy, which should be considered in future studies.

B. Discussion about Power Consumption and E2E Delay

Two other important parameters in IoT, and WSN applications are the amount of consumed power by the nodes, and the time it takes for a packet to be delivered to the destination.



(a) Power Consumption (mW) (b) End-to-End Delay (Seconds)

Figure 13: Power Consumption, and E2E Delay analysis for the Routing Mechanisms in Presence of Different Mobility Models.

These parameters are typically managed via routing policies. According to Fig. 13, the average amount of consumed power by the nodes, and the E2E delay are illustrated for all of the routing policies, and mobility models. Based on the results, we could observe that OMARPL has provided the minimum amount of power consumption. As it was discussed earlier, this routing mechanism is also providing the highest attachability. With higher amount of attachability, more number of nodes will be connected to the network. Therefore, less efforts would be required for joining the network, and fewer control packet is expected for having a stable connection. Furthermore, more number of nodes will be engaged in the process of path selection. Accordingly, the path diversity will be improved in the network. As a result, the routing mechanism will have more options to select the preferred parent, and optimize the intended parameter in the network.

Providing higher attachability in one hand, and considering the remaining energy and Estimated Life-Time *(ELT)* of the nodes as two of the many routing metrics in its objective function, OMARPL has been able to significantly reduce the power consumption by up to 41%, and 22%, compared with ORPL, and MARPL, respectively. In contrast, ORPL showed a poor performance in terms of attachability in mobile applications. Hence, in most of the time, the mobile nodes are disconnected from the network trying to join it (more power consumption will be imposed to the nodes). Nevertheless,

when a node joins the DODAG, due to using ETX as its parent selection metric, it selects a path with minimum number of attempts for having a successful transmission. Therefore, ORPL has provided faster packet delivery among the others. Based on these experiments, we could conclude that selecting the appropriate routing metric along with considering mobility-aware aspects of the mobile applications could lead into a high attachable routing mechanism, which optimizes the intended metric.

VII. Conclusion and Future Studies

In this paper, we have introduced attachability; a novel metric for evaluating the capability of routing protocols in assisting the mobile or stationary nodes in joining the network, and maintaining their connection via its routing policies. It is believed that this newly defined metric, would have a more pivotal role than the PDR in reporting the overall reliability of a routing mechanism. Hence, in addition to PDR, the attachability should be also considered as part of the reliability calculation for a routing policy. The amount of provided attachability by a routing protocol is measured via Markov chain analysis and the sample frequency-based estimation technique. Based on our evaluations, which have been conducted on a mobile RPL-based IoT infrastructure, attachability is highly dependent on the routing metrics, and the path selection procedure of a routing policy. According to our evaluations, among three versions of RPL, including ORPL, MARPL, and OMARPL, OMARPL has been able to improve the amount of attachability in mobile networks by up to 42%, and 10% compared with ORPL, and MARPL, respectively. Due to the direct relation between attachability and path diversity in the network, employment of appropriate metrics in the routing policy along with considering mobility-aware aspects of the mobile applications could lead into a high attachable routing mechanism, which could optimize the intended metrics as much as possible. As a future study, we need to extend the evaluation of attachability to more number of routing mechanisms in IoT, and WSN, to pave the way for developing and introducing novel attachable routing mechanisms for emerging mobile wireless applications.

References

[1] J. Henkel *et al.*, "Ultra-low power and dependability for iot devices (invited paper for iot technologies)," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*. IEEE, 2017, pp. 954–959.

[2] B. Safaei *et al.*, "Effects of rpl objective functions on the primitive characteristics of mobile and static iot infrastructures," *Microprocessors and Microsystems*, vol. 69, pp. 79–91, 2019.

[3] E. Ancillotti *et al.*, "Reliable data delivery with the ietf routing protocol for low-power and lossy networks," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 3, pp. 1864–1877, 2014.

[4] B. Safaei *et al.*, "Impacts of mobility models on rpl-based mobile iot infrastructures: An evaluative comparison and survey," *IEEE Access*, vol. 8, pp. 167 779–167 829, 2020.

[5] M. Bouaziz *et al.*, "Ema-rpl: Energy and mobility aware routing for the internet of mobile things," *Future Generation Computer Systems*, vol. 97, pp. 247–258, 2019.

[6] R. Ullah *et al.*, "Energy and congestion-aware routing metric for smart grid ami networks in smart city," *IEEE access*, vol. 5, pp. 13 799–13 810, 2017.

[7] K. Kritsis *et al.*, "A tutorial on performance evaluation and validation methodology for low-power and lossy networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1799–1825, 2018.

[8] H.-S. Kim *et al.*, "Load balancing under heavy traffic in rpl routing protocol for low power and lossy networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 4, pp. 964–979, 2016.

[9] M. Xue and S. Roy, "Spectral and graph-theoretic bounds on steady-state-probability estimation performance for an ergodic markov chain," *Journal of the Franklin Institute*, vol. 348, no. 9, pp. 2448–2467, 2011.

[10] T. Clausen *et al.*, "The lightweight on-demand ad hoc distance-vector routing protocol-next generation (loadng)," *draft-clausen-lln-loadng-09 (work in progress)*, 2013.

[11] C. Perkins *et al.*, "Rfc3561: Ad hoc on-demand distance vector (aodv) routing," 2003.

[12] P. Thubert *et al.*, "Rpl: Ipv6 routing protocol for low power and lossy networks," *RFC 6550*, 2012.

[13] M. Bouaziz *et al.*, "Ekf-mrpl: Advanced mobility support routing protocol for internet of mobile things: Movement prediction approach," *Future Generation Computer Systems*, vol. 93, pp. 822–832, 2019.

[14] H. Fotouhi *et al.*, "mrpl: Boosting mobility in the internet of things," *Ad Hoc Networks*, vol. 26, pp. 17–35, 2015.

[15] A. Mohammadsalehi *et al.*, ""armor: A reliable and mobility-aware rpl for mobile internet of things infrastructures"," *IEEE Internet of Things Journal*, 2021.

[16] S. Murali and A. Jamalipour, "Mobility-aware energy-efficient parent selection algorithm for low power and lossy networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2593–2601, 2018.

[17] S. R. Lalani *et al.*, "Refer: A reliable and energy-efficinet rpl for mobile iot applications," in *Proceedings of the 3rd CSI/CPSSI IEEE International Symposium on Real-Time and Embedded Systems and Technologies (RTEST)*.

[18] F. Osterlind *et al.*, "Cross-level sensor network simulation with cooja," in *proceedings of the 31st IEEE conference on Local computer networks*. IEEE, 2006, pp. 641–648.

[19] Z. J. Haas, "A new routing protocol for the reconfigurable wireless networks," in *Proceedings of ICUPC 97-6th International Conference on Universal Personal Communications*, vol. 2. IEEE, 1997, pp. 562–566.

[20] P. Levis *et al.*, "The trickle algorithm," *Internet Engineering Task Force, RFC6206*, 2011.

[21] C. R. Mesh. (2018) "cisco resilient mesh". [Online]. Available: https://www.cisco.com/, Accessed: [Mar. 2, 2019].

[22] N. Ye *et al.*, "Robustness of the markov-chain model for cyber-attack detection," *IEEE Transactions on Reliability*, vol. 53, no. 1, pp. 116–123, 2004.

[23] P. Guttorp and V. N. Minin, *Stochastic modeling of scientific data*. CRC Press, 1995.

[24] V. Peterka, "Bayesian approach to system identification," in *Trends and Progress in System identification*. Elsevier, 1981, pp. 239–304.

[25] D. Mizutani *et al.*, "Improving the estimation of markov transition probabilities using mechanistic-empirical models," *Frontiers in Built Environment*, vol. 3, p. 58, 2017.

[26] N. Lethanh *et al.*, "Determination of markov transition probabilities to be used in bridge management from mechanistic-empirical models," *Journal of bridge engineering*, vol. 22, no. 10, p. 04017063, 2017.

[27] G. Roelfstra *et al.*, "Condition evolution in bridge management systems and corrosion-induced deterioration," *Journal of Bridge Engineering*, vol. 9, no. 3, pp. 268–277, 2004.

[28] T.-C. Lee *et al.*, "Estimating the parameters of the markov probability model from aggregate time series data," 1970.

[29] G. Bolch *et al.*, *Queueing networks and Markov chains: modeling and performance evaluation with computer science applications*. John Wiley & Sons, 2006.

[30] J.-J. Lee and J. Lim, "Cognitive routing for multi-hop mobile cognitive radio ad hoc networks," *Journal of Communications and Networks*, vol. 16, no. 2, pp. 155–161, 2014.

[31] C. Liu *et al.*, "The research on wireless sensors network reliability," in *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*. IEEE, 2008, pp. 1–4.

[32] J. Liu *et al.*, "A framework for information propagation in mobile sensor networks," in *2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems*. IEEE, 2013, pp. 214–221.

[33] A. Kalita and M. Khatua, "Channel condition based dynamic beacon interval for faster formation of 6tisch network," *IEEE Transactions on Mobile Computing*, vol. 20, no. 7, pp. 2326–2337, 2020.

[34] ——, "Adaptive control packet broadcasting scheme for faster 6tisch network bootstrapping," *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17 395–17 402, 2021.
[35] ——, "Autonomous allocation and scheduling of minimal cell in 6tisch network," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12 242–12 250, 2021.
[36] C. Vallati *et al.*, "Improving network formation in 6tisch networks," *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 98–110, 2018.
[37] Y. Al-Nidawi and A. H. Kemp, "Mobility aware framework for timeslotted channel hopping ieee 802.15. 4e sensor networks," *IEEE Sensors Journal*, vol. 15, no. 12, pp. 7112–7125, 2015.
[38] A. Kalita and M. Khatua, "Opportunistic transmission of control packets for faster formation of 6tisch network," *ACM Transactions on Internet of Things*, vol. 2, no. 1, pp. 1–29, 2021.
[39] F. Righetti *et al.*, "An evaluation of the 6tisch distributed resource management mode," *ACM Transactions on Internet of Things*, vol. 1, no. 4, pp. 1–31, 2020.
[40] M. Vučinić *et al.*, "Trickle-d: High fairness and low transmission load with dynamic redundancy," *IEEE internet of things journal*, vol. 4, no. 5, pp. 1477–1488, 2017.
[41] S. Chowdhury *et al.*, "Noncooperative gaming for energy-efficient congestion control in 6lowpan," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4777–4788, 2020.
[42] A. Kalita and M. Khatua, "A non-cooperative gaming approach for control packet transmission in 6tisch network," *IEEE Internet of Things Journal*, 2021.
[43] H. Verma *et al.*, "Buffer-loss estimation to address congestion in 6lowpan based resource-restricted 'internet of healthcare things' network," *Computer Communications*, vol. 181, pp. 236–256, 2022.
[44] R. J. Ellison *et al.*, "Survivable network system analysis: A case study," *IEEE software*, vol. 16, no. 4, pp. 70–77, 1999.
[45] S. Peng *et al.*, "Quantitative evaluation model for survivability in large-scale manets based on reliability theory," in *2008 The 9th International Conference for Young Computer Scientists*. IEEE, 2008, pp. 432–438.
[46] G. Kalogridis and R. Lin, "Connection availability and transient survivability analysis in wireless ad-hoc networks," in *Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*, 2009, pp. 188–195.
[47] T. Zhang *et al.*, "Multipath routing and mptcp-based data delivery over manets," *IEEE Access*, vol. 8, pp. 32 652–32 673, 2020.
[48] H. Yuan *et al.*, "Dynamic route selection for vehicular store-carry-forward networks and misbehaviour vehicles analysis," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2018, pp. 1–5.
[49] L. Zhang *et al.*, "Cooperative positive orthogonal code-based forwarding for multi-hop vehicular networks," *IEEE transactions on wireless communications*, vol. 13, no. 7, pp. 3914–3925, 2014.
[50] Z. Zou and M. Johansson, "Minimum-energy packet forwarding over lossy networks under deadline and reliability constraints," in *2012 10th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*. IEEE, 2012, pp. 224–231.
[51] H. Xia *et al.*, "An attack-resistant trust inference model for securing routing in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7108–7120, 2019.
[52] M. Salehi *et al.*, "On the effect of black-hole attack on opportunistic routing protocols," in *Proceedings of the 12th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks*, 2015, pp. 93–100.
[53] M. E. Moe *et al.*, "Tsr: Trust-based secure manet routing using hmms," in *Proceedings of the 4th ACM symposium on QoS and security for wireless and mobile networks*, 2008, pp. 83–90.
[54] S. Yousefi *et al.*, "Mobile agents for route planning in internet of things using markov decision process," in *2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*. IEEE, 2018, pp. 303–307.
[55] Y. Zhai *et al.*, "A dht and mdp-based mobility management scheme for large-scale mobile internet," in *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2011, pp. 379–384.
[56] S. Sati *et al.*, "Dynamic replication control strategy for opportunistic networks," in *2017 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2017, pp. 1017–1023.
[57] Q. Wang and S. Zhang, "Analytic latency model for message dissemination in opportunistic networks," in *2016 IEEE Wireless Communications and Networking Conference*. IEEE, 2016, pp. 1–7.
[58] P. Chen and S. Sastry, "Latency and connectivity analysis tools for wireless mesh networks." in *ROBOCOMM*, 2007, p. 33.
[59] F. Despaux *et al.*, "Extracting markov chain models from protocol execution traces for end to end delay evaluation in wireless sensor networks," in *2015 IEEE World Conference on Factory Communication Systems (WFCS)*. IEEE, 2015, pp. 1–8.
[60] K. Chen and H. Shen, "Dtn-flow: Inter-landmark data flow for high-throughput routing in dtns," *IEEE/Acm Transactions on Networking*, vol. 23, no. 1, pp. 212–226, 2014.
[61] R. Ruiz *et al.*, "Considering scheduling and preventive maintenance in the flowshop sequencing problem," *Computers & Operations Research*, vol. 34, no. 11, pp. 3314–3330, 2007.
[62] M. Anityasari *et al.*, "The role of warranty in the reuse strategy," in *Advances in Life Cycle Engineering for Sustainable Manufacturing Businesses*. Springer, 2007, pp. 335–340.
[63] R. Kassan *et al.*, "Reliability assessment of photovoltaic wireless sensor networks for forest fire propagation detection," *International Journal of Modelling and Simulation*, vol. 38, no. 1, pp. 50–65, 2018.
[64] A. Dunkels *et al.*, "Contiki-a lightweight and flexible operating system for tiny networked sensors," in *proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*. IEEE, 2004, pp. 455–462.
[65] M. R. Palattella *et al.*, "Standardized protocol stack for the internet of (important) things," *IEEE communications surveys & tutorials*, vol. 15, no. 3, pp. 1389–1406, 2012.
[66] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile computing*. Springer, 1996, pp. 153–181.
[67] B. Liang and Z. J. Haas, "Predictive distance-based mobility management for PCS networks," in *IEEE INFOCOM'99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No. 99CH36320)*, vol. 3. IEEE, 1999, pp. 1377–1384.
[68] F. Bai *et al.*, "IMPORTANT: A framework to systematically analyze the Impact of Mobility on Performance of RouTing protocols for Adhoc NeTworks," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)*, vol. 2. IEEE, 2003, pp. 825–835.

Bardia Safaei received his Ph.D. degree in computer engineering from Sharif University of Technology, Tehran, Iran, in 2021. He was a member of Dependable Systems Laboratory (DSL) during 2014–2017, and Embedded Systems Research Laboratory (ESRLab) during 2017-2021. As a Ph.D. visiting researcher, he was with the Chair for Embedded Systems (CES) at Karlsruhe Institute of Technology (KIT), Germany from 2019 to 2020. Currently, he is a faculty member at the department of computer engineering at Sharif University of Technology, Tehran, Iran, where he is the director of the Reliable, and Durable IoT Applications & Networks (RADIAN) Laboratory. He is honored to be selected as a member of the national elites foundation from 2016 to 2020. He received the ACM/SIGAPP student award in the 34th ACM/SIGAPP Symposium on Applied Computing (SAC'19). Dr. Safaei has served as a reviewer in several prestigious international journals and conferences, such as IEEE Transactions on Mobile Computing (TMC), IEEE Transactions on Vehicular Technology (TVT), IEEE Communications Magazine, ACM Transactions on Storage (ToS), Elsevier Microprocessors and Microsystems, Telecommunication Systems (TELS), ACM/IEEE Design Automation Conference (DAC), IEEE Sensors Conference, and IEEE World Forum on Internet of Things (WF-IoT). His research interests include power efficiency and dependability challenges in Internet of Things, Wireless Sensor Networks, Mobile Ad-hoc Networks, and Fog computing.

Hossein Taghizade received his B.Sc. degree in Computer Engineering from Ferdowsi University, Mashhad, Iran, in 2017, and his M.Sc. degree in Computer Architecture Engineering from Sharif University of Technology, Tehran, Iran, in 2021. He is a member of Embedded Systems Research Laboratory (ESR-LAB) in the computer engineering department at Sharif University of Technology. His main research interests include energy-efficiency and reliability in Internet of Things (IoT), embedded systems, wireless sensor networks, and machine learning.

Amir Mahdi Hosseini Monazzah received his Ph.D degree in computer engineering from the Sharif University of Technology, Tehran, Iran, in 2017. He was a member of the Dependable Systems Laboratory from 2010 to 2017. As a Visiting Researcher, he was with the Embedded Systems Laboratory, University of California, Irvine, CA, USA from 2016 to 2017. As a postdoc fellow he was with the school of computer science, institute for research in fundamental sciences (IPM), Tehran, Iran from 2017 to 2019. He is currently a faculty member of the School of Computer Engineering, Iran University of Science and Technology (IUST), Tehran, Iran. His research interests include investigating the challenges of emerging nonvolatile memories, hybrid memory hierarchy design, and IoT applications.

Kimia Talaei Khoosani received her B.Sc. degree in computer engineering from Sharif University of Technology, Tehran, Iran. Currently, she is a Master of Science student in computer engineering at University of Toronto, Canada. She was a member of the Embedded System Research Laboratory (ESRLab) at the department of computer engineering, Sharif University of Technology from 2019 to 2020. Her major research interests include Internet of Things, Wireless Sensor Networks, embedded systems and computer architecture.

Parham Sadeghi received his B.Sc. degree in computer hardware engineering from the University of Tabriz, Iran in 2015, and his M.S. degree also in computer architecture engineering from University of Isfahan, Iran in 2018. He is currently pursuing his Ph.D. degree in computer engineering with the Sharif University of Technology, Tehran, Iran. His current research interests include analytical modeling, in-memory processing and low-power embedded systems.

Aliasghar Mohammadsalehi received his B.Sc. degree in computer engineering from Sharif University of Technology, Tehran, Iran, in 2017, where he also received his M.Sc. degree in computer engineering in 2020. He is currently pursuing his Ph.D. degree in electrical and computer engineering at Rutgers University, New Jersey, USA. As a graduate research assistant, he is currently with the Wireless Information Network Laboratory (WINLAB), Rutgers University, where he is conducting research on designing next-generation wireless networks, and developing machine learning-based techniques in the context of edge computing. He is also experienced in cooperating with industry for more than five years. His main research interests include energy-efficiency and reliability in Internet of Things (IoT), Wireless Networks, and Cyber-Physical Systems (CPS).

Jörg Henkel (Fellow, IEEE) received the Diploma degree and the Ph.D. degree (summa cum laude) from the Technical University of Braunschweig. Before that, he was a Research Staff Member with NEC Laboratories, Princeton, NJ, USA. He is currently the Chair Professor for Embedded Systems with the Karlsruhe Institute of Technology. His research interests include co-design for embedded hardware/software systems with respect to power, thermal, and reliability aspects. He has received six best paper awards throughout his career from, among others, ICCAD, ESWeek, and DATE. For two consecutive terms, he served as the Editor-in-Chief for the ACM Transactions on Embedded Computing Systems. He is also the Editor-in-Chief of the IEEE Design&Test Magazine. He is/has been an Associate Editor for major ACM and IEEE Journals. He has led several conferences as a General Chair incl. ICCAD, ESWeek. He serves as a Steering Committee chair/member for leading conferences and journals for embedded and cyber-physical systems. Prof. Henkel coordinates the DFG program SPP 1500 ”Dependable Embedded Systems”. He is a Site Coordinator of the DFG TR89 collaborative research center on ”Invasive Computing”. He is the Chairman of the IEEE Computer Society, Germany Chapter.

Alireza Ejlali received the PhD degree in computer engineering from Sharif University of Technology in, Tehran, Iran, in 2006. He is currently an associate professor of computer engineering at Sharif University of Technology. From 2005 to 2006, he was a visiting researcher in the Electronic Systems Design Group, University of Southampton, Southampton, United Kingdom. In 2006, he joined Sharif University of Technology as a faculty member in the department of computer engineering and from 2011 to 2015 he was the director of Computer Architecture Group in this department. His research interests include low power design, real-time embedded systems, and fault-tolerant embedded systems.