Detection of Sinkhole Attacks for Supporting Secure Routing on 6LoWPAN for Internet of Things

Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri Santos
NR2 – Informatics Department – UFPR – Brazil
emails: {cavcervantes, dap10, michele, aldri}@inf.ufpr.br

***Abstract*—The Internet of Things (IoT) networks are vulnerable to various kinds of attacks, being the sinkhole attack one of the most destructive since it prevents communication among network devices. In general, existing solutions are not effective to provide protection and security against attacks sinkhole on IoT, and they also introduce high consumption of resources de memory, storage and processing. Further, they do not consider the impact of device mobility, which in essential in urban scenarios, like smart cities. This paper proposes an intrusion detection system, called INTI (Intrusion detection of SiNkhole attacks on 6LoWPAN for InterneT of ThIngs), to identify sinkhole attacks on the routing services in IoT. Moreover, INTI aims to mitigate adverse effects found in IDS that disturb its performance, like false positive and negative, as well as the high resource cost. The system combines watchdog, reputation and trust strategies for detection of attackers by analyzing the behavior of devices. Results show the INTI performance and its effectiveness in terms of attack detection rate, number of false positives and false negatives.**

I. Introduction

The Internet has been adopted not only by people but also by devices with some intelligence, i. e., with computational capacities that enable them, among other tasks, to send and receive information over the network. Due to advances in technology and the reduction of computational devices, such devices have become more affordable and available to the general public. The concept of the Internet of Things (IoT) [1] has emerged based on these advances. IoT is a hybrid and open network that integrates heterogeneous devices named smart objects (things), like appliances, books and cars, and other objects that do not usually belong to computation interacting with computers, sensors, cell phones, PDAs, others devices. These devices seek to share information, data and resources, acting and reacting to situations and changes in the environment [2].

The IoT is the result of a technological revolution that represents the future of computing and communication tasks. Therefore, its aim is to enable the integration and unification of all objects and communication systems that surround us. Also, IoT has a number of application domains, such as automotive, healthcare, logistics, environmental monitoring, and many others. IoT envisions an age where billions of things (devices) will be connected to the Internet and communicating with each others, and this means that a large amount of data will be exchanged and processed. Technologies as IEEE 802.15.4, 6LoWPAN [3], and RPL [4] make possible the creation of real applications connected to the IoT. However, in reason of the increase of intelligent devices and the mobility of some of these, IoT is exposed to several vulnerabilities found in a variable communication infrastructure. Most IoT devices possess limited computational resources, like low power, limited capacity processing, storage, loss of links connection and other features. Such limitations becomes IoT vulnerable to routing attacks [5], being the sinkhole attack one of the most destructive routing attacks. An sinkhole attacker aims to attract the greatest amount of traffic in a given area harming the reception of data on collection point. Thus, it compromises the reliability and integrity of the data sent by the devices (node).

In general, there are many studies that quantify the impact of sinkhole attacks on networks like MANETs, WSNs and VANETs [6], [7]. However, these solutions cause other problems, called **adverse effects**, on the network , such as high rates of false positives and false negatives, high energy consumption, slow system performance, among others. Moreover, few studies handles the protection and security of information transmissions in the IoT [8], [9]. Further, such studies are limited in terms of the dynamic network topology because they do not consider the device mobility; and that characteristic essential to its application by people and objects. The intrusion detection systems (IDS) to have improved safety on attacks and threats to computer networks. Some proposals employ watchdog strategies for local detection of the attacking node [10], being they able to listen and analyze packets transmitted by neighbor nodes. Other studies have applied reputation and trust [11] mechanism on the networks to identify the origin of the threat. Those mechanism are efficient and help to reduce the impact of network attacks. However, those strategies have not been applied in IoT.

This work presents a system to identify the presence of attacks sinkhole within the routing service IoT, named INTI (***I**nstrusion detection for SiN**k**hole attacks over 6LoWPAN for Interne**T** of Th**I**ngs*). INTI aims to prevent, detect and isolate the effects of the attack sinkhole in the routing, while mitigating adverse effects. It combines watchdog, reputation and trust strategies for detection of attackers by analyzing the behavior of each node. Simulation results show that INTI ensures a detection rate of at least 90% with fixed devices and 70% with mobile devices in presence of malicious nodes.

This paper is organized as follows: Section II presents the related works. Section III defines the model and assumptions taken by the INTI. Section IV describes the INTI system and details its functions and modules. Section V shows the evaluation of INTI on the detection of attacks. Finally, Section VI presents the conclusions and future work.

II. Related Work

Several works found in the literature have addressed the detection of sinkhole attacks on wireless networks, such as

978-3-901882-76-0 @2015 IFIP

wireless sensor networks (WSNs), vehicular ad hoc networks (VANETs) and mobile ad hoc networks (MANETs). Those works employ a diversity of techniques, including clustering, cooperative sensing, geostatistical monitoring, fuzzy logic, and others. In [12], the authors propose an IDS for WSN, in which master nodes monitor the communication and analyze collected data employing *fuzzy logic* to detect sinkhole attacks. In [6], the authors describe a hybrid IDS based on clusters also for WSNs. The IDS applies a combination of anomaly detection, supported by a vector machine (SVM), and signatures. This system performs a training process, in which each IDS agent trains the SVM, and performs a voting majority decision to indicate the suspect nodes. In addition to the well-known limitations of systems using signatures and training phases, the IDS based on fuzzy logic and the hybrid one generate a high rate of false positives and false negatives. In [7], the authors present a IDS that employs mobile agents for the detection of sinkhole attacks. Those agents apply a navigation algorithm in which a mobile agent must provide network information when visiting each node in the networks. This approaches fails because it is very hard to discriminate fake from legitimate paths in the network and the attempt to differentiate them may generate a high overhead in the network.

In [11], it is proposed a mechanism based on **reputation** to identify malicious nodes in a WSN. It considers the formation of clusters of nodes, in which the leader analyzes the data collected from the nodes into the cluster to localize a malicious event, using data redundancy. Similarly, In [10], the authors propose a system to detect selfish nodes in VANETs, consisting of two phases: motivation to nodes cooperate and use of **watchdogs**. The first aims at motivating network nodes to act in a cooperative manner using incentives, and the second phase employs **watchdogs** to detect selfish nodes, based on cooperative evidences, that increase the likelihood of detection. However, these strategies, despite of being efficient and effective in VANETs, must be used together with other approaches to really ensure safe communication environment for the IoT.

There are few studies about the protection and security in data transmission in the context of IoT. In [8], the authors present SVELTE, an IDS that cope with different attacks, including sinkhole, selective forwarding and sybil. The centralized system defines three modules: mapping (6Mapper), intrusion detection and a mini-firewall to routing attacks. In [9], the authors describe Ebbits, a system that employs a component to monitor the network traffic in order to perform an analysis and detect misbehaving nodes. Ebbits detects DoS (denial of service) attacks in 6LoWPAN networks. Although, Ebbits fits to most of the IoT features, it does not consider node mobility and it presents limitations in analyzing node behaviors. Moreover, SVELTE and Ebbits result in high resource consumption, producing low network and system performance.

III. System Model

This section describes the communication and attack models assumed on the IoT network. The communication model consists of two levels: inter and intra cluster communication among physical network nodes. The first one corresponds to the communication established on the several clusters, and the second one comprises the formation of the clusters. This communication model considers also the mobility and the data routing of the devices.

A. Physical network, Communication and Attack Models

Physical network model: The physical network corresponds to a set P of n devices (nodes) identified by $\{n_1, n_2, n_3, ..., n_i\}$ where $n_i \in P$. Each node n_i has a unique physical address that determines its identification (ID). The transmission node occurs through wireless medium using an asynchronous channel subjects to packet loss due to noise and node mobility. The nodes are composed of different resources, like memory size and battery. Further, all nodes has the same transmission range, can move in different directions, and are arranged virtually in clusters.

The network devices are classified as free nodes, cluster member nodes, associated nodes, leader nodes and base station. Free nodes do not belong to any cluster and can move within the network area. The member nodes belong to a cluster and send their information to leader nodes in time intervals. The leader nodes receive information from member nodes and associated nodes sending it torwards the base station. The associated nodes forward information between clusters in order to facilitate the data routing and the connection among different clusters. The base station receives all the collected data. Figure 1 illustrates the network entities and their relationships.

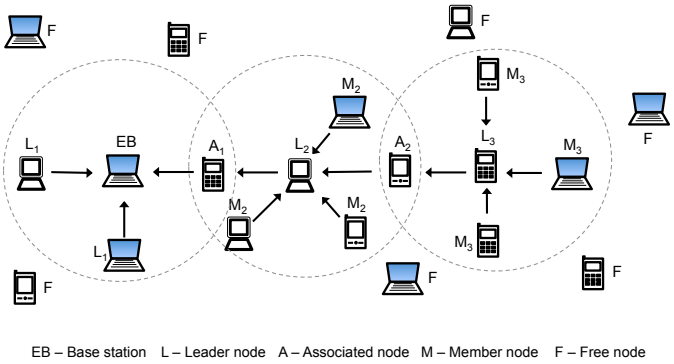


Figure 1. Entities in the network

Communication model: The devices communication model employs the RPL protocol (*IPv6 Routing Protocol for Low power and Lossy Networks*), which respects the resource limitations of IoT devices. However, as RPL only works on static devices and environments [4], it was developed a new routing protocol inspired on RPL, which takes into account both the devices mobility and the cluster formation.

Attack model: as each node is responsible for sending and forwarding data packets, sinkhole nodes can try to play in given time as leader, associated or member nodes. The sinkhole attack is viewed as the most destructive of all routing attacks in wireless networks [5]. In this type of attack, the attacker announces to its neighbors that it knows the shortest path to a desired destination. It aims to attract the traffic in certain area to discard the packets and harm the network communication.

IV. THE INTI ARCHITECUTURE

This section shows the architecture of INTI - (***I**nstrusion detection for Si**N**khole attacks over 6LoWPAN for Interne**T** of Th**I**ngs*). The INTI system considers the devices mobility, as well as the attackers can play different roles in the network, such as free node, member node, leader node. It offers properties of **self-organization** and **self-repair** on the network. The first property aims at the coordination and cooperation of the devices to the network configuration. The second property allows the detection of suspicious nodes and cluster regrouping in order to maintain the network stability. INTI runs on four modules: cluster configuration, routing monitoring, attack detection and attack isolation, as showed in Figure 2.

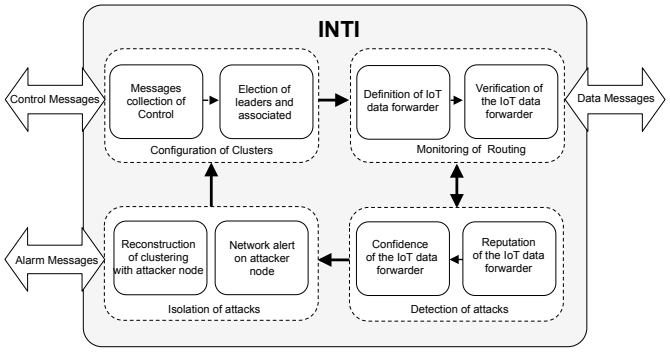


Figure 2. The INTI system architecture

A. Configuration of clusters

This module defines a leader-based hierarchy establishing node clustering to ensure scalability and extend the lifetime of the network. Nodes are classified as members, associated and leaders depending on their network functions. The role of each node can change over time in reason of the network reconfiguration due to node mobility or an attack event.

Initially all nodes in the network play as free node, collecting and transmitting control data. The nodes send data via broadcast to establish the exchange of control messages. These message enable nodes to estimate the amount of neighboring nodes in order to elect leaders. The free nodes are classified as candidate to leaders when they have the greatest amount of neighboring nodes in relation to others. After the election of leaders, the clustering are defined. At this stage, leaders await the decision of their neighbors (free nodes) for joining to one of the leaders to form the cluster. Once established the clusters, leaders check if one of their cluster nodes (member node) received more than one message from different leaders. If a member node receives more than one message, this node will be the associated one, which is able to interconnect clusters. In case there are two members nodes within the same area, it will be considered as associated node that one with the highest energy content (*IE*) which is: $IEi = \frac{TEr_i}{TEc_i}$, where TEr_i represents the total energy remaining from the same node and TEc_i is the total energy consumed by the node n_i.

INTI applies the Beta Probability Density Function, denoted by $Beta(p|\alpha, \beta)$ [13], to establish the probability of the future behavior of a node based on its past results, and thus estimating the state of each node behavior. Additionally, the beta (α, β) parameters are constantly updated determining the behavior of a node. Equation 1 defines the Beta function, where p is the probability of α and $(1-p)$ is the probability of β.

$$\begin{aligned} Beta(p|\alpha,\beta) &= \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \\ &= \frac{p^{\alpha-1}(1-p)^{\beta-1}}{B(\alpha,\beta)} \end{aligned} \quad (1)$$

$$Where: 0 \leq p \leq 1 \quad e \quad \alpha, \beta > 0$$

The probability density and its statistical expectation are based on the Beta function. It is represented by the integral defined by: $B(\alpha,\beta) = \int_0^1 t^{\alpha-1}(1-p)^{\beta-1}dt$. The variable *status* (*St*) stores the nodes behavior, determining the operation mode of a node in the transmission of messages. $St = \frac{\alpha}{\alpha+\beta}$. This value takes into account the likelihood of future hope *E (p)*, which is calculated from the density function of Beta.

The reconfiguration of the clusters occurs when a node fails, when it leaves a cluster or when a sinkhole attack occurs. When a leader node is affected by one of these issues, two actions can happen: the election of a new leader into the cluster or the member nodes affected regroups in the neighboring clusters. In case of an associated node be affected, other member node can be selected as associated since it is within the common area. Otherwise, if both cluster leaders are within the same transmission radius, a fusion of clusters happens considering the highest number of member nodes that each group has. That aims to minimize the number of leaders.

B. Monitoring routing

INTI defines a monitoring module to count the transmission number of input and output performed by a node responsible for forwarding messages. For this, the "observer" node monitors the number of transmissions performed by a "top" node, responsible for forwarding its messages. A node is called top node if it has a (*rank*) lower. Thereafter, its estimates the amount of transmission inputs and outputs performed. If the amount of incoming streams is equal to the number of output streams, the node is good. Otherwise, it is assumed that is happening any deviations from the normal operation. Figure 3 illustrates the operation of monitoring and data routing from other clusters. Figure 3 (a) shows three clusters and the way through which data will be sent to the destination. Figure 3 (b) shows part of the network where $(n_2, n_3,$ and, $n_4)$, cluster members, send and monitor its own data, the node (n_{14}) acts in the role of leader, it will receive and forward the data from its own cluster and the neighboring cluster.

C. Detection of the attacker

INTI identifies and reveals the identity of a sinkhole attacking node. The module of attacker detection performs two kinds of evaluations. These evaluations estimate the reputation and trust of the node to detect sinkhole attacks. Such assessments maintain continuously the security and integrity of the node.

Reputation is the belief or perception that nodes establish by iterations, actions or information exchange among them.

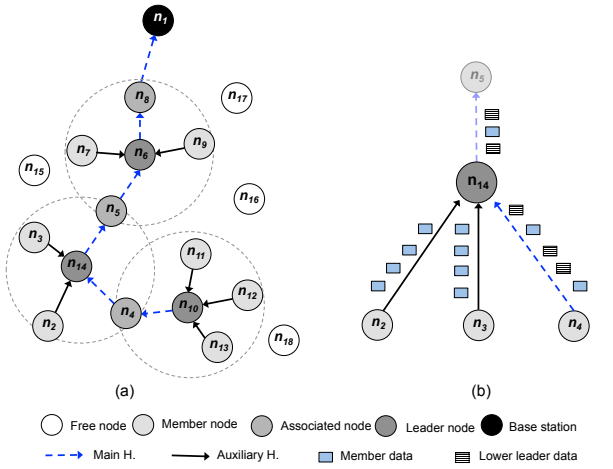


Figure 3. Example of monitoring and routing

These iterations, based on the monitoring operations, are achieved by direct way, i.e. inside of a cluster, or indirect way, i.e. between two clusters [14]. The use of the *Beta* (α,β) distribution is essential to reputation and trust of nodes. The advantage of this distribution is that the parameters are continuously updated. The INTI system calculates three predictions: uncertainty (u), belief (b) and disbelief (d) using the *Beta* (α,β) distribution in order to represent the node reputation. All nodes perform these calculations. The calculation of these predictions $(u, b, d) \in (0, 1)^3 : u+b+d = 1$ respectively. Uncertainty (u) is the normalized variance of the *Beta* (α,β) distribution, which is calculated according to: $u = \frac{12*\alpha*\beta}{(\alpha+\beta)^2*(\alpha+\beta+1)}$. Certainty is $(1-u)$, which can be divided into b and d according to their proportion of iterations. Whereas confidence transmission of two nodes is defined by $\frac{\alpha}{(\alpha+\beta)}$. The belief b calculation is given by: $b = \frac{\alpha}{(\alpha+\beta)}(1-u)$. Finally, the calculation of disbelief (d) is achieved by: $d = (1-u) - b = \frac{\beta}{(\alpha+\beta)}(1-u)$.

After the calculation of the predictions obtained (u, b, d), it is possible to achieve the node reputation. This value considers its own communication iterations and predictions computed by itself based on the *status* sent by a member node to its leader. Thus, each node propagates its *status* (*St*) on **its behavior in the transmission of messages** for the calculation of its reputation. These values are input data employed by the detection module to apply Theory *Dempster-Shafer* to increase detection probability and reduce false alarms. Reputation is a continuous value within the limits P [0,1], if the reputation value is greater than or equal to 0.5, the node is assumed as "good"; otherwise, it considered as an attacker. A node $n_i : \Omega\{T, \overline{T}\}$, where Ω hypothesis has three (H): $H = T$ is that n_i is good, $\overline{H} = \overline{T}$ shows n_i not good and $U = \Omega$ where n_i is what is good or not good. For example, if the leader node L_1 states that a node member m_2 is good, then its basic probability assignment is represented by Equation 2.

$$\begin{aligned} m_2(H) &= b \\ m_2(\overline{H}) &= 0 \\ m_2(U) &= 1-b \end{aligned} \tag{2}$$

If L_1 discloses a broadcast message to state that the member node m_2 is not good, and its probability assignment is represented by Equation 3.

$$\begin{aligned} m_2(H) &= 0 \\ m_2(\overline{H}) &= b \\ m_2(U) &= 1-b \end{aligned} \tag{3}$$

The previous probabilities determined by L1 for m_2 takes into account the (*St*) of m_2. The use of probabilities by L1 relative to node m_2 is showed by Equation 4. Where K is the normalization of beliefs represented by $K = \sum_{L\cap M=\emptyset} m_1(L)m_2(M)$. The reputation value is given by $m_1(H) \oplus m_2(H)$ ranging a continuous value between $0 \leq m_2 \leq 1$. This result considers $m_2 < 0,5$ as a bad reputation. Otherwise, m_2 is a good node.

$$\begin{aligned} m_1(H) \oplus m_2(H) &= \frac{1}{K}[m_1(H)m_2(H) + m_1(H)m_2(U) + m_1(U)m_2(H)] \\ m_1(\overline{H}) \oplus m_2(\overline{H}) &= \frac{1}{K}[m_1(\overline{H})m_2(\overline{H}) + m_1(\overline{H})m_2(U) + m_1(U)m_2(\overline{H})] \\ m_1(U) \oplus m_2(U) &= \frac{1}{K}[m_1(U)m_2(U)]. \\ Where: K = \; & m_1(H)m_2(H) + m_1(H)m_2(U) + m_1(U)m_2(H) + \\ & m_1(\overline{H})m_2(\overline{H}) + m_1(\overline{H})m_2(U) + m_1(U)m_2(\overline{H}) + \\ & m_1(U)m_2(U) \end{aligned} \tag{4}$$

The next step is the calculation of the Confidence (*C*). It consists of the honesty relation that an entity has to another. This calculation considers two values (γ, δ) represented by Equation 5. The value u computes the number of iterations performed between n_i and n_j, which is represented by m: $u = 1 - \frac{1}{m}$, where u has values between $0 \leq u \leq 1$. This value is a factor to find the confidence to a node.

$$\gamma = u\gamma + R \quad ; \quad \delta = u\delta + (1-R) \tag{5}$$

Equation 6 obtains the confidence value of a node. This value ranges between [0,1] and the average value is 0,5. If the confidence value is greater than 0,5 the node is good; otherwise, the node is an attacker. The reputation and trust values need to be updated consistently for sinkhole detection.

$$C = \mathbf{E}(Beta(\gamma+1, \delta+1)) = \frac{\gamma+1}{\gamma+\delta+2} \tag{6}$$

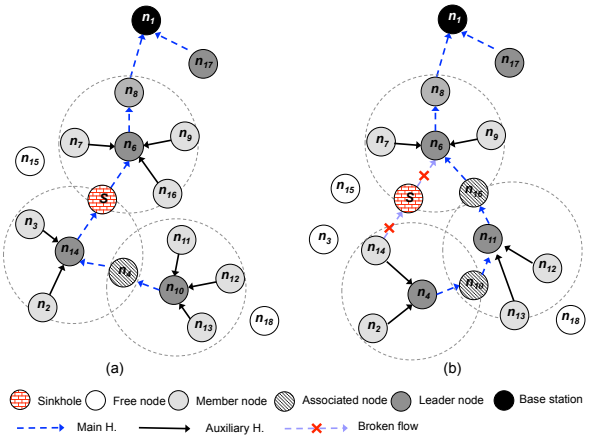


Figure 4. Detection of sinkhole attack

Figure 4 (a) illustrates a node n_5 acting as an associated node, turns into a sinkhole attacker node. Thus, affecting the

routing messages of the cluster nodes. This figure also shows nodes playing different functions due to their mobility on the network. Figure 4 (b) shows how an attacker is detected by n_{14}, as well as n_{14} discloses the attacker identity and forwards a cluster reconstruction message for isolating the attacker and keeping the stability in the communication among the clusters.

D. Isolation of attacker

This module isolates a sinkhole node after its detection. For this, the node that has detected the sinkhole attack generates and propagates an alarm message in *broadcast* with the purpose of alerting the neighboring nodes. Moreover, this node promotes the isolation of the attacker by sending a message of restoration to its neighbors. The main data propagated in th restoration message consists of the *cluster rank*, in order to allow nodes of same rank start a regrouping.

There are three ways to isolate a sinkhole: (i) when a sinkhole node is a member node: the own leader will isolate such node; (ii) when the sinkhole node acts as leader; in this case, the member nodes isolate the sinkhole node or if there is a node associated, it will isolate the attacker; (iii) when the sinkhole node acts as associated node, it will be isolated by the leader node, with the largest *rank*, breaking thus communication with the attacker. It is also important to verify if exists within the cluster,other associated nodes with the lowest *rank*, so that they can forward messages to the destination node. Otherwise, the leader will spread a message of restoration to its members to join the neighboring clusters.

V. Analysis

The INTI system was implemented in the simulator Cooja [15] because the SVELTE system is also implemented at the same simulator. INTI is evaluated and compared to SVELTE in terms of its effectiveness and effeciency to mitigate sinkhole attacks. The evalution scenario consists of 50 nodes, some fixed and others mobile, which represents the average number of users transiting on a street. These users have wireless devices such as cell phones, PDAs, laptops, and transit in an enclosed area. The scenario comprises a realistic urban environment of a street [16], where there are different types of objects and devices. These users may be pedestrian, people running, cyclists, and even cars that move with speeds between 0 m/s to 6.94 m/s (10mk/h). The number of sinkhole nodes ranges between 10 and 15, respectively 20 % and 30 % of all nodes. Each node uses a wireless communication channel, following the propagation model (*Medium Unit Disk Graph* (UDGM)), and the motion model *RandomWaypoint* in regions of 80 *x* 80 *m* and 100 *x* 100 *m*. INTI employs as routing protocol an extension of the RPL protocol to allow clustering. The node range varies from 30 to 40 *m* and they employ the UDP protocol. The simulation time is 1500s. The results are the average of 35 simulations and confidence interval of 95 %. Four metrics are employed in order to assess the INTI and SVELTE system under sinkhole attacks: *detection rate* (T_{det}), the false negative (Tx_{Fn}), false positive (Tx_{Fp}) and delivery rate ($Tx_{Delivery}$).

Detection rate of sinkhole attack (T_{det}) accounts the attacks correctly identified. This metric is achieved by Eq. 7, where *X* means the total number of iterations of attacker identified by the system, given in the form of *X=(d, c)*, where *d* is the value of the detection performed, and *c* is the current behavior of the node $n_i \in P$.

$$T_{det} = \frac{\sum D_i}{|X|} \forall_i \in X, \quad \text{where} \quad D_i = \begin{cases} 1, & \text{if} \quad d_i = c_i, \\ 0, & \text{if} \quad d_i \neq c_i. \end{cases} \tag{7}$$

False negative rate (Tx_{Fn}) indicates the amount of times that attacks were considered by the system as trusted. This metric is obtained by Eq. 8, where *X* counts the total number of iterations performed by the system, and T_{det} is the detection rate of sinkhole attacks achieved by Eq. 7.

$$Tx_{Fn} = |X| - T_{det} \tag{8}$$

False positive rate (Tx_{Fp}) determines the amount of times that the system has detected a sinkhole attack as negative. Tx_{Fp} is calculated by Eq. 9, and *Z* is the set of iterations of normal nodes, in the form *Z = (d, c)*, where *d* means the value of the detection performed by system and *c* is the real condition of the node $n_i \in P$, where *c= 1* is an attacker and *c= 0* is not.

$$Tx_{Fp} = \frac{\sum Dp_i}{|Z|} \forall_i \in Z, \quad \text{where} \quad Dp_i = \begin{cases} 1, & \text{if} \quad d_i = c_i, \\ 0, & \text{if} \quad d_i \neq c_i. \end{cases} \tag{9}$$

Delivery rate of packets ($Tx_{Delivery}$) determines the number of data packets successfully received. $Tx_{D}elivery$ consists the number of received packets received divided by the number of packets originated by the source.

$$Tx_{Delivery} = \frac{NreceivedPackets}{NsentPackets} X100 \tag{10}$$

A. Results

INTI and SVELTE on a fixed scenario had T_{det} 92% and 90% respectively, as shown in Fig. 5(a). In a mobile scenario, Fig. 5(b), the SVELTE T_{det} decreased to 24% and the INTI T_{det} is over 70%. SVELTE had a lower T_{det} because it does not consider the node mobility. Fig. 6 and Fig. 7 show the results for Tx_{Fn} and Tx_{Fp} metrics. Fig. 6 shows one comparison between INTI and SVELTE when varying the speed of network nodes. Where the rate of false negatives obtained by INTI in a fixed setting is 8%. That means almost all sinkhole nodes are detected. The failure on the sinkhole detection may be due to the detection autonomy, which allows each node to account packets transmitted by another node, in which it is forwarder. Thus, nodes can delay to identify a sinkhole attack. For a scenario with mobile nodes, the number of false negatives obtained by INTI is 28% and SVELTE is 38%, Fig.6(b). This increase of the false negative number happens due to the dynamics on network nodes.

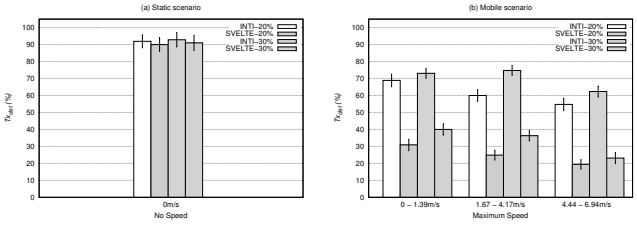


Figure 5. T_{det} under sinkhole attacks

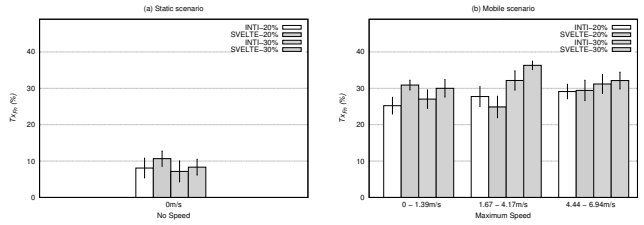


Figure 6. Tx_{Fn} - INTI and SVELTE under sinkhole attacks

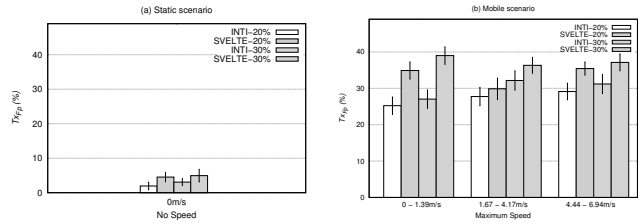
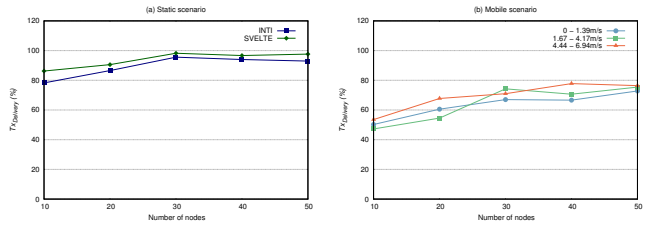


Figure 7. Tx_{Fp} - INTI and SVELTE under sinkhole attacks



In Fig. 7(a), the Tx_{Fp} obtained by INTI with fixed nodes is less than 3%. While SVELTE achieved 4%. the Tx_{Fp} obtained by INTI with mobile nodes, Fig. 7 (b), is less than 30% and SVELTE is 39%. The detection failure can happen if nodes delay the packet forwarding, being briefly considered attackers.

Figure 8. $Tx_{Delivery}$ - INTI and SVELTE

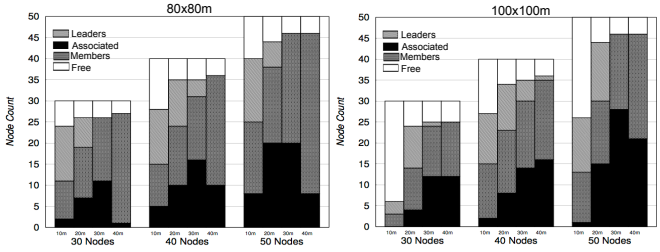


Figure 9. Roles assumed by nodes in the INTI

In the fixed scenario, SVELTE has a higher delivery rate $Tx_{Delivery}$, reaching 99% upon delivery of the IoT data, exceeding the 95% achieved by INTI, as shown in Fig. 8(a). It is also possible to observe that INTI begins with a delivery rate of 79% achieving 95% after. This variation is due to the low amount of nodes within the established area. Thus, with increasing number of nodes increases the delivery rate. Fig. 8(b) shows only the INTI evaluation, since SVELTE does not take into account the node mobility. This graph considers different speeds previously defined. As it possible to note early INTI has a delivery rate of more than 55%, and as increases the number of nodes and the speed, INTI achieves a delivery rate of more than 75%. Fig. 9 shows the number of leaders, members, associateds and free nodes achieved during the INTI simulation, considering different areas and ranges.

VI. Conclusion

This paper introduced the INTI system for detection and isolation of sinkhole attacks in IoT. INTI establishes dynamic clustering to support IoT data transmission and observe the behavior of router nodes in the forwarding task. The behavior of suspicious nodes is detected by reputation and trust mechanisms. Simulation results show that INTI achives a sinkhole detection rate up to 92% on fixed scenario and 75% in mobile scenario. Further, INTI showed a low rate of false positives and negatives than SVELTE. As future work, we will assess the INTI performance to detect other types of attacks in IoT.

References

[1] S. Haller, "The things in the internet of things," vol. 5, 2010, p. 26.

[2] H.-D. Ma, "Internet of things: Objectives and scientific challenges," in *Journal of Computer Science and Technology*, vol. 26, no. 6. China: Springer USA, 2011, pp. 919–924.

[3] J. Hui, D. Culler, and S. Chakrabarti, "6LoWPAN: Incorporating IEEE 802.15. 4 into the IP architecture–internet protocol for smart objects (IPSO) alliance, white paper# 3, january 2009," 2009.

[4] M. A. C. S. L. Korbi, I.E. Ben Brahim, "Mobility enhanced RPL for wireless sensor networks," in *Network of the Future (NOF), 2012 Third International Conference*. IEEE, 2012, pp. 21–23.

[5] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the rpl-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[6] H. Sedjelmaci and M. Feham, "Novel hybrid intrusion detection system for clustered wireless sensor network." in *International Journal of Network Security & Its Applications*, vol. 3, no. 4, 2011.

[7] K. C. N. Sheela, D. and G. Mahadevan., "A non cryptographic method of sinkhole attack detection in wireless sensor networks," in *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on*. Tamil Nadu, Chennai: IEEE Security, 2011, pp. 527–532.

[8] S. Raza, L. Wallgren, and T. Voigt., "Svelte: Real-time intrusion detection in the internet of things." USA: Elservier, 2013, pp. 2661 – 2674.

[9] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6lowpan based internet of things," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*. IEEE, 2013, pp. 600–607.

[10] O. A. Wahab, H. Otrok, and A. Mourad, "A cooperative watchdog model based on dempster–shafer for detecting misbehaving vehicles," *Computer Communications*, vol. 41, pp. 43–54, 2014.

[11] C. R. Perez-Toro, R. K. Panta, and S. Bagchi, "Rdas: reputation-based resilient data aggregation in sensor network," in *Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010 7th Annual IEEE Communications Society Conference on*. IEEE, 2010, pp. 1–9.

[12] S. Y. Moon and T. H. Cho., "Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks." in *International Journal of Computer Science and Network Security*. Coreia: IEEE Computer Society, 2009, pp. 118–122.

[13] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks," *Computer Communications*, vol. 31, no. 17, pp. 3941–3953, 2008.

[14] F. Li and J. Wu., "Mobility reduces uncertainty in MANETs." in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE Computer Society, 2007, pp. 1946–1954.

[15] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *Local Computer Networks, Proceedings 2006 31st IEEE Conference on*. Flórida, USA: IEEE Computer Society, 2005, pp. 641–648.

[16] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, "Convergence of MANET and WSN in IoT urban scenarios," vol. 13, no. 10. IEEE, 2013, pp. 3558–3567.