A Context-Dependent Trust Model for the MAC Layer in LR-WPANs

Bernardo M. David, Beatriz Santana, Laerte Peotta, Marcelo D. Holtz, Rafael Timóteo de Sousa Jr
Electrical Engineering Department, ENE
University of Brasilia
Brasília/Brasil
{bernardo.david,beatriz.santana,peotta,holtz,desousa}@redes.unb.br

Abstract - **Low rate wireless personal networks are vulnerable to several attacks focused on the Media Access Layer. Malicious or faulty nodes can subvert CSMA/CA and GTS allocation algorithms, achieving MAC unfairness in order to obtain higher medium access priority or to interrupt legitimate communication, ultimately leading to Denial-of-Service. While there exist secure protocol frameworks for LR-WPANs and diverse countermeasures against these attacks, most of them do not fit the usual computational and power supply constraints of LR-WPAN nodes, which require less computationally intensive methods such as trust models. We extend a bayesian trust model designed to detect such attacks by introducing context-dependent parameters and a flexible ageing factor which enable adaptive control of the proposed trust model based on specific context attributes and on changing network conditions.**

KEYWORDS - SENSOR NETWORK; TRUST, MAC LAYER, LR-WPAN

I. INTRODUCTION

Low rate wireless personal networks (LR-WPANs) [4] are being adopted in several applications, among them wireless sensor networks (WSN) and other systems which require low power consumption. Protocol stacks for WSNs (such as ZigBee) and proper Ad-Hoc routing protocols can be used on top of IEEE 802.15.4 MAC and physical layers in order to fit the power supply and processing performance constraints of WSN nodes [16]. In such resource constrained scenarios, the waste of power and cpu cycles caused by denial of service (DoS) attacks poses a serious threat. Furthermore, the overall network performance degradation causes delays unacceptable in real-time applications, commonly served by LR-WPANs.

Several kinds of DoS attacks have been proposed against WSNs [15], affecting diverse layers. For the most part these attacks consist in performing irregular operations in the network or application layers, which generate traffic or noise patterns that can be identified and used to detect malicious nodes; hence, secure routing protocols and trust models based on the Network layer may be applied to hinder such attacks. However, the exploitation of MAC layer vulnerabilities, e.g. unfairness, does not clearly expose the offending nodes because it is achieved through modifications to CSMA/CA parameters and medium access methods, so that traffic patterns associated with attacks resemble legitimate communication or medium access contention between honest nodes.

Most of the secure protocols and security models proposed for WSNs in current literature provide authentication, integrity and confidentiality services mainly in the Network and Application layers. However, these frameworks tend to increase processing loads and packet sizes (resulting in longer transmission periods per packet), consequently shortening battery life [10] while not properly addressing attacks focused on the MAC layer. As an efficient alternative to the high cpu loads, packet overhead and consequent reduced battery life inherent to purely cryptographic solutions, trust-based security mechanisms were developed for Ad-Hoc networks and, in particular, for LR-WPANs. Trust-based models provide the level of security required by various applications without significant increases in transmission time, processing loads or memory usage, fitting the resources constraints of WSN nodes. Thus, attacks which explore MAC unfairness or subvert the MAC layer can be efficiently detected and mitigated by trust models based on this layer's data.

A bayesian trust model capable of detecting and mitigating DoS attacks based on MAC unfairness was introduced in [1]. However, it was stated as an open problem the efficient control of trust value convergence, evidence ageing and parameters which depend on attributes of an specific application. We extend this model proposing a new trust model with a flexible ageing factor and context-dependent parameters which makes it adaptable to different specific applications. We analyse how the ageing factor and context-dependent parameters affect the proposed model's overall behaviour, demonstrating its efficiency and adaptability. Similarly to the original model [1], the bayesian trust model proposed by us is also suitable for enforcing GTS allocation policies and may serve as a component of a more comprehensive Multi-Layer trust model.

The rest of this paper is structured as follows: In section II, we present an overview of common DoS attacks focused on the MAC layer of LR-WPANs. In section III, we discuss the trust model for the MAC layer presented in current literature. In section IV, we describe the proposed trust model in detail. In section VI, we present simulation results regarding our trust model's performance with several ageing factors and context-dependent parameters in different scenarios. Finally, in section VI, we conclude with a summary of our results and directions for future research.

II. DENIAL OF SERVICE ATTACKS IN THE IEEE 802.15.4

MAC Layer

Denial of Service (DoS) results from any action which prevents the network from functioning correctly or in a timely manner. The objective of a DoS Attack is to render the LR-WPAN inaccessible or degrade its performance for honest nodes [3]. The shared nature of the wireless medium makes wireless networks specially vulnerable to monitoring and tampering by any adversary within transmission range, making them more vulnerable to such attacks. In face of the high power consumption of radio devices, WSN nodes operate in low-power mode (i.e. with radio turned off) for most of the time as a method to save energy, only activating its radio transceiver when there's data being received or queued for transmission, operations that consume much more power than regular data acquisition and processing. A DoS attack in the MAC layer may force nodes to keep the radio in receive mode for long periods, or, in the worst case, retry several retransmissions before finally dropping a packet. These anomalous operations caused by DoS attacks decrease battery life and waste processing resources, thus posing a serious threat to resource-limited WSNs [13].

Although the MAC layer is not affected by as much vulnerabilities as the Network Layer, it figures as an important target, considering that its anomalous activities might not be detected by security solutions placed in upper layers and that it controls the radio power modes [4]. We focus on DoS attacks which consist of bypassing the MAC protocol priority scheme, mainly by cheating when negotiating channel access (exploiting MAC unfairness). This way a malicious node can keep the other nodes from transmitting while maintaining legitimate communication, making it difficult to identify this attack. Other approaches to compromising the MAC Layer, such as Collision and Exhaustion attacks, can be efficiently detected and mitigated, as they generate identifiable traffic patterns.

A. DoS attack based on MAC Unfairness

Both the attack and definitions discussed in this section were introduced in [1]. MAC fairness is achieved when nodes have the same medium access priority. Put differently, the MAC sublayer is fair when the bandwidth is equally allocated to each contending node over similar periods of time. The fairness of a MAC protocol may be verified by observing the network on a short-term or a long-term basis [8]. Although the MAC sublayer achieves long-term fairness it might present short-term unfairness, which degrades real-time applications performance [7]. MAC unfairness happens in scenarios where a node or a group of nodes captures and monopolizes the channel for a long period. It can be achieved by malicious nodes that cheat when contending for access, subverting multiple access protocols so as to gain access before other nodes.

Attacks based on MAC unfairness are extremely effective because they do not generate any easily identifiable traffic pattern, thus being indistinguishable from legitimate communication. Furthermore, being targeted at the MAC layer, these attacks can not be thwarted by security solutions based on upper layers. Simulation results in [17] show that, even though packet delivery rate (PDR) is not significantly affected by MAC unfairness for moderate traffic loads, the packet delivery latency (PDL) tends to grow for any traffic load. An adversary could build on the increased latency to perform attacks against other protocols and layers, such as Network Layer adhoc routing protocols.

LR-WPANs operate in both beacon and non-beacon enabled modes, each requiring different multiple access protocols for channel access. Non-beacon-enabled mode uses CSMA-CA while beacon-enabled mode uses slotted CSMA-CA during the contention access period (CAP), since it provides better performance for synchronized networks. Attack methods differ from one scenario to another.

B. Non-beacon-enabled Mode

In the CSMA-CA multiple access algorithm, a node vying for access will first wait for a random backoff period of $P = random(2^{BE} - 1) * aUnitBackoffPeriod$ symbols (where $BE = macMinBE$ in the first iteration of the algorithm) and then perform the Clear Channel Assessment (CCA) procedure. If the channel is idle the node proceeds and transmits its data, whereas, if the channel is busy, it will make BE=BE+1, wait for another random period P and retry (performing again the CCA). The IEEE 802.15.4 macMaxCSMABackoffs parameter controls how many times this process will be repeated before CSMA-CA terminates with a CHANNEL_ACCESS_FAILURE status, which will be recieved in the MLME-COMM-STATUS.indication primitive issued by the MLME.

An adversary who wants to disrupt the network would perform a DoS attack against the PAN or local coordinators, depriving the ordinary nodes, which are reduced function devices (RFDs), of communication. In multihop networks, such an attack could completely isolate one region of the network if there aren't any alternative routes (coordinators) outside the attacker's transmission range.

A simple method to execute this attack is to perform the CCA repeatedly, without waiting for the backoff period, until the channel is found to be idle and capturing the channel as soon as possible. The attacker could then keep the channel busy by transmitting a large sequence of messages. This would prevent the other nodes that were contending for access from transmitting their data, causing delays. It is important to notice that, if this attack is repeated too frequently, it will resemble a deceptive jamming attack, becoming easier to detect, even though it is exploring a MAC unfairness vulnerability. Another way to achieve similar results is to wait for arbitrarily small backoff times before performing the CCA. An attacker using the latter method would not always capture the channel, but it still increases PDL and makes attack detection more difficult.

C. Beacon-enabled Mode

In beacon-enabled mode two beacons delimit a superframe structure, which is divided into 16 time slots by default and further broken down into Contention Access Period (CAP), Contention Free Period (CFP) and inactive period. Slotted CSMA-CA is used during CAP and no multiple access algorithm is used during CFP, instead, nodes allocate

Guaranteed Time Slots (GTS), during which they have total priority to transmit data to a coordinator. A GTS may consist of up to seven time slots and is allocated by sending a GTS request during the CAP and waiting for the coordinator's response in the next beacons.

A beacon-enabled mode DoS attack targeting the CAP is achievable by capturing the channel immediately after a beacon is received. A cheating node may simply wait for the arrival of a beacon packet and then start transmitting immediately by skipping backoff and CCA processes. The attacker can then maintain its control of the channel by transmitting successive messages as in non-beacon-enabled mode.

It is also interesting to target the CFP, causing the coordinator to waste resources and GTS dependent applications to fail. If an adversary can capture the channel during the CAP, it can issue one or more GTS request commands to allocate the possible maximum number of GTS and then keep the channel busy, so as to prevent other nodes from also allocating GTS. The coordinator would probably allocate all the CFP in the next superframe to the malicious node, that could simply send nothing or send random data, forcing the coordinator to receive and process it.

In both attacks, the other nodes will get a CHANNEL_ACCESS_FAILURE status when issuing GTS request commands or contending for channel access. When all GTSs have been allocated the GTS request commands issued by legitimate nodes will receive a MLME-GTS.confirm primitive with a status of DENIED.

III. Countermeasures: the trust-based approach

Several countermeasures against DoS attacks in WSNs have been suggested, including secure protocol suites such as SPINS [11], which focus on the Network layer, and TinySec [6], a Link layer solution. However, most of these solutions rely on cryptographic functions to provide confidentiality, integrity and authentication services. As stated earlier, cryptography centered consume too much of a WSN node's limited resources and secure protocol control data and encrypted information in general represent and overhead that increases packet size, consequently increasing transmission time. The heavy processing loads and longer transmission times inherent to current solutions contribute to dramatically decrease the node's battery lifetime. Moreover, most of the current solutions are not capable of detecting MAC unfairness. In face of such disadvantages, specific less computationally intensive trust models offer an efficient countermeasure against DoS attacks in the MAC layer.

A trust-based MAC layer security protocol was proposed in [12]. This protocol addresses authentication and confidentiality problems in the network and MAC layers of wireless ad-hoc networks. It provides a trust mechanisms which enable nodes to select the most trustworthy routes, instead of simply choosing the shortest path. However, the trust model employed in this solution does not effectively take into consideration prior information obtained about the nodes, nor does it offer parameters which control how much prior information is considered in the trust calculation process and the importance given to such information. Moreover, even though this protocol offers a seemingly efficient solution for authentication and confidentiality on the Link-layer and Mac sub-layer applying a block cipher in CBC-X mode, the authors do not present formal proofs of security.

A bayesian trust model based on MAC Layer data capable of detecting MAC unfairness and the attacks that exploit it was proposed in [1].Processing MAC sublayer operational data such as CSMA-CA completion status with the Beta Reputation System [5] combined with a modified communication trust model [9] enables the PAN and local coordinators of a IEEE 802.15.4 network to unfair or malicious nodes. In the model poposed in [1], coordinators receive MAC sub-layer operational data from sensor nodes and compare it with prior information on the node's behavior to calculate a node's trust value. By cross-referencing data collected from different nodes in different points of the network it is possible to obtain reliable information about a potential malicious node. This approach reduces the processing load in the nodes, transferring most of the necessary calculations to the coordinators. This model is able to detect unfair nodes in the MAC layer, so that it can be used to hinder attacks where a node tries to retain control of the transmission medium in order to increase its bandwidth or simply disrupt legitimate communication.

However, through careful analysis of the simulation results presented, it is possible to notice that the trust of a dynamic node (i.e. a node that oscillates between honest and malicious behaviors) takes several time periods to converge to its new value when a change of behavior occurs, which is a serious problem in many applications where adversaries may adaptively change their behavior. Furthermore, apart from the convergence factor, there is no other parameter to control how fast the trust value changes. The model also lacks parameters to control how much of the collected evidence is considered in the trust value update process, which is important in dynamic environments and serves as another method to control trust value convergence.

In the simulation results analysed we consider a sensor network consisting of 10 nodes equally distant from the PAN Coordinator in star topology transmitting constant bit rates during intervals smaller than the reporting period P_C (in this model, the nodes report on their status every P_C seconds enabling the Coordinator to update their trust values). The convergence factor is set to $c = 0.5$ and the trust values T_{c_i} between the coordinator and five of the network nodes are observed against a time interval of $1000 * P_C$ in order to verify the convergence speed and behavior of the trust model. Interesting results arise in the dynamic adversaries scenario, where a node performs the attack for a period $400 * P_C$ and then starts behaving honestly while another node that was previously behaving honestly becomes malicious. The attack performed is the one introduced in [1] and described in the previous section.

The case of a dynamic adversary is shown in Figure 5. In this scenario the model's behavior is analysed in a more realistic dynamic setting, with nodes alternating between honest and malicious behavior in the course of the simulation. While nodes 2,3 and 4 behave honestly during the whole simulation, node 5 performs the attack until period 400 ($time = 400 * P_C$) and then starts behaving honestly. Conversely, node 1 behaves honestly until period 400 ($time = 400 * P_C$) and then starts performing the attack.

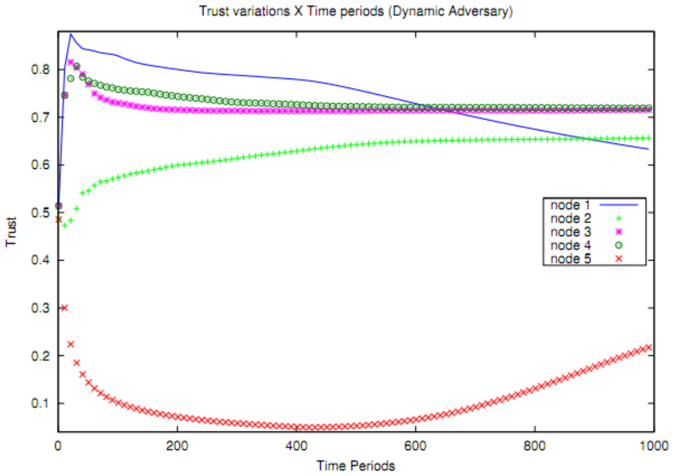


Figure 1: Trust between the PAN coordinator and the nodes T_{c_i} versus time periods P_C in the case of dynamic adversaries. Node 5 becomes honest and node 1 becomes malicious at period 400.

The graphic in Figure 5 shows that the trust T_{C_i} of all nodes oscillates until period 100, after which it is possible to observe a clear tendency to converge to certain values, and becomes stabilized around period 400. After the instant $400 * P_c$, T_{c_1} decreases slower than it increased until $400 * P_c$, and so does T_{c_5}, that increases slower than it decreased before. This characteristic is inherent to bayesian statistical models, which take into account previous knowledge on the variable that is being estimated. Even though the observed behavior is expected in bayesian statistical models, it renders the original trust model ineffective in certain dynamic adversary settings.

The trust value of node 1 T_{c_1} only equals the trust value of honest nodes after 200 periods of dishonest activity and, at the end of the simulation (period 1000), the difference between T_{c_1} and $T_{c_{2,3,4}}$ is approximately 0.1. After period 400, T_{c5} starts increasing significantly and, at period 1000, reaches the value of approximately 0.2. The curves pertaining T_{c1} and T_{c5} indicate that the model considers too much prior information in the trust value update process. This fact is clearly verified by observing that $T_{c1} >> T_{c5}$ even after the nodes swap their behavior for 600 periods, reflecting the tendency observed until period 400, before which node 1 behaves honestly and node 5 behaves maliciously. In order to properly detect attacks in dynamic scenarios the model should have parameters which enable efficient adaptive configuration of trust value convergence rates and control of how much prior information is to be considered in trust value calculation.

IV. A Context-Dependent Trust Based Approach to DoS Attacks Mitigation in WSNs

Various trust models have been proposed for different layers of ad-hoc networks, providing security and resiliency at several levels and yielding interesting results. Even though most of the trust models for ad-hoc networks in current literature focus on the network layer, a MAC layer based bayesian trust model was introduced in [1]. This model efficiently identifies and mitigates attacks that involve subverting media access algorithms and protocols (generating MAC unfairness) without the cryptography overhead. Through the evaluation of MAC layer data in a modified communication trust and Beta reputation model, it is possible to obtain a trust value for each node which indicates the probability of this node being malicious or honest, enabling further security mechanisms to detect malicious nodes and act against them.

Communication trust is a concept introduced in [9] and modelled mathematically using evidence theory and the Beta reputation system [5]. It was originally defined as the trust value between nodes based on their cooperation in routing messages around the network, being modified in [1] to reflect the trust of reduced function nodes in relation to the PAN coordinator or local coordinators based on MAC layer operational data.

In the trust model introduced in [1] data regarding CSMA-CA completion status and GTS allocation are fed into the Beta Reputation System [5] combined with the modified communication trust model, enabling the PAN and local coordinators of a LR-WPAN to determine if a node is unfair or malicious and take defensive actions against it. We propose a Bayesian trust model where coordinators receive MAC sub-layer operational data from sensor nodes and compare it with past information collected over time to calculate a node's trust value. By cross-referencing data collected from different nodes in different points of the network it is possible to obtain reliable information about a potential malicious node. This approach reduces the processing load in the nodes, making the coordinators responsible for most of the calculations.

This model is able to detect MAC unfairness and the offending nodes, so that it can be used to thwart attacks where a node tries to gain control of the transmission media in order to increase its bandwidth or simply disrupt legitimate communication. However, in order to be fully efficient, this trust model should be combined with an energy efficient method of authentication for verifying the source of MLME status messages (which will be further discussed in the next session), decreasing the probability that malicious nodes forge such messages, causing honest node's trust values to decrease.

The model introduced in [1] can also be used as basis for a GTS allocation algorithm, providing information regarding the GTS allocation history of all nodes.

Even though this model was proven to be efficient against static adversaries, the simulation results analysed in the previous section show that it is not appropriate for settings where dynamic adversaries adaptively alter behavior between malicious and honest. As stated in the previous section, the model should incorporate parameters which enable efficient adaptive configuration of trust value convergence rates and control on the quantity of prior information which is considered in trust value calculation. Such characteristics can be added to the original model by introducing the context-dependent parameters, ageing factor and normalization procedure presented in [14]. The proposed context-dependent bayesian trust model is based on the same principles introduced in [1] (including the protocol modifications), while introducing the proper control parameters.

The MLME Status Reporting protocol introduced in [1], described in the next subsection, is incorporated in the proposed model.

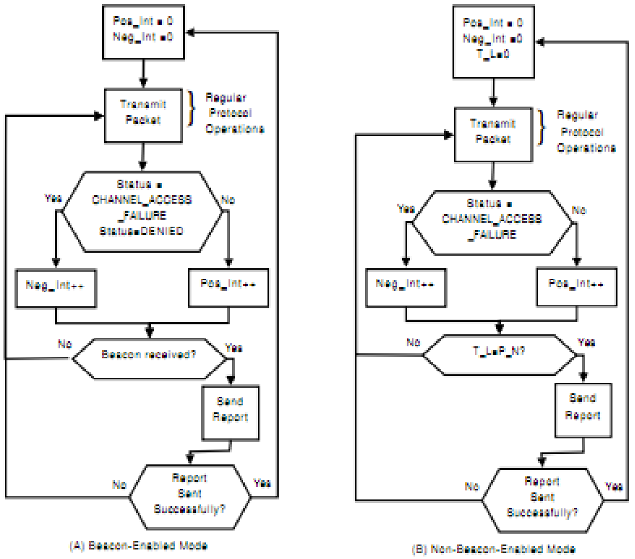
A. *Protocol Modifications: MLME Status Reporting*

Nodes must report the status of the MLME-COMM-STATUS.indication and MLME-GTS.confirm primitives issued by the MLME to the PAN Coordinator after each channel access and GTS requests. A node keeps two records regarding interactions, namely Negative_Interactions (Neg_Int) and Positive_Interactions (Pos_Int), that it will report to the Coordinator. This minor addition to the protocol enables the Coordinator to calculate trust values based on the behavior of all nodes in the network and also transfers processing loads from the nodes to the Coordinator, which usually has more resources. It is important to notice that these modifications may be implemented in the Application Layer through the use of SCSS Layer functionality, making it easy to adapt current networks to operate with this trust model.

In beacon-enabled mode a node increments the Neg_Int record if it receives MLME-COMM-STATUS.indication or MLME-GTS.confirm primitives with a status of

CHANNEL_ACCESS_FAILURE or DENIED and increments the Pos_Int record if these primitives have any other status values. It will wait for a random period and try to report the interactions records each time a beacon is received. If the report transmission succeeds then both records are cleared whereas if the node is unable to send the report it will keep incrementing the records and will wait for the next beacon before retrying, as illustrated in Figure 2 (A).

In non-beacon-enabled mode a node increments the Neg_Int record if it receives MLME-COMM-STATUS.indication primitive with a status of CHANNEL_ACCESS_FAILURE and increments the Pos_Int record if this primitive has any other status values. In order to keep the node (loosely) synchronized with the coordinator, both will keep a timer T_L (started and adjusted by the node at the moment it joins the network) and the node will send its reports after periods of P_C time units, where P_C is a predefined constant. If the node can't send the report it will keep incrementing the records and will wait for P_C time units before retrying, as illustrated in Figure 2 (B).



(A) Beacon-Enabled Mode (B) Non-Beacon-Enabled Mode

Figure 2: MLME Status Reporting Algorithm

The coordinator receives the reports and marks them with a time stamp before analyzing the information. It uses the current beacon sequence number as the time stamp in beacon-enabled mode and the current time (based on T_L) in non-beacon-enabled mode respectively. The reports are temporarily stored in the following format:

TABLE 1: REPORT FORMAT

time stamp	*Neg_Int*	*Pos_Int*
1 Octets	2 Octets	2 Octets

B. *The Proposed Trust Model for WSNs*

Using the Beta Reputation System [5] and the concept of Communication Trust for WSNs presented in [9] it is possible to define a model where the reputation of node N_i maintained by the PAN Coordinator C is given by the Beta probability distribution. Introducing context-dependent parameters [14] into the original model [1] the reputation of a node N_i in relation to its coordinator is given by:

$$R_{Ci} = Beta(\alpha_{Ci} + \alpha_0, \beta_{Ci} + \beta_0) \tag{1}$$

where α_{Ci} and β_{Ci} are respectively the number of positive and negative feedbacks about a node N_i received from the other nodes of the network as seen by the coordinator and $Beta(\alpha,\beta)$ is the Beta probability distribution. The values α_0 and α_0 (which will be defined later) represent the initial trustworthiness of an unknown node. In this context, positive feedbacks represent fair MAC protocol operation while negative transactions represent potentially malicious or unfair MAC protocol operation. Thus, the trust between the PAN coordinator and the nodes T_{Ci} (representing the probability of a node behaving honestly) is defined as:

$$T_{Ci} = E(R_{Ci}) = E[Beta(\alpha_{Ci}+\alpha_0,\beta_{Ci}+\beta_0)] = \\ = \frac{\alpha_{Ci}+\alpha_0}{\alpha_{Ci}+\beta_{Ci}+\alpha_0+\beta_0} \tag{2}$$

When a new node N_j joins the PAN, the Coordinator sets $\beta_{Aj} = \alpha_{Aj} = 0 = \beta_{Cj} = \alpha_{Cj}$. This means that the new node has equal probability of being honest or malicious, which is a natural assumption as there's no previous information regarding its behavior, as seen by the coordinator. The coordinator continuously waits for an adjustable period of time $P_C = t_2 - t_1$ and starts the trust update process. During this process the reports received during the last time slot are taken into account for calculating the new values for α_{Ai} and β_{Ai}, which represent respectively the number of positive and negative feedbacks about a node N_i received from the other nodes of the network $N_{j\neq i}$. First the Coordinator calculates threshold values $Thres_S^i$ and $Thres_F^i$ using the reports R_i^t received from each node during the period P_C and updates the variables α_{Ai} and β_{Ai} according to the following logic:

$$\begin{aligned}
&Sr_i^t > Thres_S^i \rightarrow \beta_{Ai}^{new} = \beta_{Ai} * a + 1, \alpha_{Ai}^{new} = \alpha_{Ai} * a \\
&Fr_i^t > Thres_F^i \rightarrow \alpha_{Ai}^{new} = \alpha_{Ai} * a + 1, \beta_{Ai}^{new} = \beta_{Ai} * a \\
&Otherwise \rightarrow \alpha_{Ai}^{new} = \alpha_{Ai} * a, \beta_{Ai}^{new} = \beta_{Ai} * a
\end{aligned} \tag{3}$$

In the expression above, a is an aging factor which controls how much of past the feedbacks will be used in the update process. If a node's success rate is bigger than $Thres_S^i$, β_{Ai} is incremented, indicating the node is acting maliciously. Conversely, if a node's failure rate is bigger than $Thres_F^i$, α_{Ai} is incremented, indicating the node is acting honestly. The values of α_{Ai} and β_{Ai} are not modified otherwise. It is important to notice that, if a node has a high Failure Rate, it means that medium access for this node is being granted in an unfair way in comparison to the other nodes, and that a high Success Rate implies that the node is granted channel access (or GTS allocation) more often than the other nodes.

Now we define the Success Rate, Failure Rate and threshold values $Thres_S^i$ and $Thres_F^i$. Once the PAN Coordinator has collected MLME Status Reports $R_i^t = (t, S_i^t, F_i^t)$ from a node $N_i, i \in \{1,...,n\}$, where n is the number of nodes in the network (for the sake of simplicity, the node's address is represented by i), it has access to the following information: S_i^t and F_i^t, which respectively represent the successful and failed transactions (either GTS or Channel Access requests) during the period P_C, where $t_1 \leq t \leq t_2$ ($t \in P_C = [t_1, t_2]$). In order to prevent malicious nodes from cheating, the coordinator compares the number of packets successfully received from each node during P_C with the reported values S_i^t and uses the larger one for subsequent calculations (denoting by S_i^t this larger value). Using these values it's possible to determine the Success Rate Sr_i^t and Failure Rate Fr_i^t of a node N_i during the period P_C:

$$Sr_i^t = \frac{S_i^t}{S_i^t + F_i^t}, where\ S_i^t, F_i^t \neq 0 \tag{4}$$

$$Fr_i^t = \frac{F_i^t}{S_i^t + F_i^t} = 1 - Sr_i^t, where\ S_i^t, F_i^t \neq 0 \tag{5}$$

The threshold values $Thres_S^i$ and $Thres_F^i$ are defined as follows:

$$Thres_S^i = \sum_{i=1}^{n} \frac{Sr_i^t}{n} + \sqrt{\sum_{i=1}^{n} \frac{(Sr_i^t - \overline{Sr_i^t})^2}{n-1}} * T_{c_i}, t \in P_C \tag{6}$$

$$Thres_F^i = \sum_{i=1}^{n} \frac{Fr_i^t}{n} - \sqrt{\sum_{i=1}^{n} \frac{(Fr_i^t - \overline{Fr_i^t})^2}{n-1}} * T_{c_i}, t \in P_C \tag{7}$$

The terms:

$$\sqrt{\sum_{i=1}^{n} \frac{(Sr_i^t - \overline{Sr_i^t})^2}{n-1}} * T_{c_i}$$

$$\sqrt{\sum_{i=1}^{n}\frac{(Fr_i^t-\overline{Fr_i^t})^2}{n-1}}*T_{c_i}$$

represent the trust value multiplied by the convergence factor and the standard deviation of Sr_i^t and Fr_i^t respectively. These threshold values are compared to the node's success and failure rates in the process of determining if a node is being unfair as described before.

After the α_{Ai} and β_{Ai} variables are updated the Coordinator can calculate the new α_{Ci} and β_{Ci} values for each node. The values α_{Ci}^{new} and β_{Ci}^{new} are obtained from the equations below, which are based on the Communication trust model presented in [9] and were first given by [2]. They have been adapted in [1] to the situation of the trust model proposed in this section, where the central Coordinator maintains Trust and Reputation information about the ad-hoc nodes.

$$\alpha_{Ci}^{new}=\alpha_{Ci}+\frac{2*\alpha_{Ci}*\alpha_{Ai}^{new}}{(\beta_{Ci}+2)*(\alpha_{Ai}^{new}+\beta_{Ai}^{new}+2)+(2*\alpha_{Ci})} \quad (8)$$

$$\beta_{Ci}^{new}=\beta_{Ci}+\frac{2*\alpha_{Ci}*\beta_{Ai}^{new}}{(\beta_{Ci}+2)*(\alpha_{Ai}^{new}+\beta_{Ai}^{new}+2)+(2*\alpha_{Ci})} \quad (9)$$

If the number of reports received exceeds a certain normalization parameter N, the values obtained for α_{Ci}^{new} and β_{Ci}^{new} are then normalized with the following equation:

$$\alpha_{Ci}^{new}=\frac{N}{\alpha_{Ci}^{new}+\beta_{Ci}^{new}}\alpha_{Ci}^{new}$$
$$\beta_{Ci}^{new}=\frac{N}{\alpha_{Ci}^{new}+\beta_{Ci}^{new}}\beta_{Ci}^{new} \quad (10)$$

The normalization parameter N determines how much of the received reports are considered in the trust update process. The normalization equations described above preserve the relative frequency of positive evidence, while scaling the total number of evidence (reports) received. The trust value of the node N_i as seen by the coordinator is finally given by:

$$T_{Ci}^{new}=E(R_{Ci}^{new})=E[Beta(\alpha_{Ci}^{new}+\alpha_0,\beta_{Ci}^{new}+\beta_0)]=$$
$$=\frac{\alpha_{Ci}^{new}+\alpha_0}{\alpha_{Ci}^{new}+\beta_{Ci}^{new}+\alpha_0+\beta_0} \quad (11)$$

$$\alpha_0=1=\beta_0 \quad (12)$$

The parameters α_0 and β_0 are introduced to represent the prior information considered about a node which has newly joined the network. Both parameters are set to 1 representing an equal probability of the node being honest or malicious. Different values may be chosen for these parameters in order to properly model the trustworthiness of an unknown node in different contexts.

Based on the trust value obtained, the PAN Coordinator can detect malicious and unfair nodes and take actions, such as: decide wether to allocate GTSs to a certain node or not, stop routing packets from unfair nodes or warn legitimate nodes and other coordinators about misbehaving nodes. We note that this protocol may be used as part of a GTS allocation policy, serving as a tool to predict and adjust the probability of GTS allocation by a specific node or to determine if certain nodes have higher GTS allocation success rates.

Because it's designed to analyse MAC sublayer information without needing to access to central routing statistics, the proposed trust model may be implemented as a distributed system between all the WSN coordinators in a large WSN, not only the PAN Coordinator. All the coordinators would share the computational loads and maintain Reputation of nodes they are responsible for, exchanging information about reputation and trust values of nodes in different zones only when needed. This characteristic makes this trust model scalable and resilient to single points of failure.

V. Simulation Analysis and Evaluation

Simulation experiments where conducted to verify the theoretic model proposed above. The proposed trust model, a subset of the IEEE 802.15.4 protocol Messages and a Two-Ray ground reflection radio propagation model were implemented using numerical programming methods in order to simulate GTS allocation requests and media access contention in Beacon-enabled mode. In this experiments we consider a sensor network consisting of 10 nodes equally distant from the PAN Coordinator in star topology transmitting constant bit rates during intervals smaller than the reporting period P_C. The trust values T_{c_i} between the coordinator and five of the network nodes are observed against a time interval of $1000*P_C$ in order to verify the convergence speed and behavior of the trust model under different context-dependent parameter values. Three different scenarios were simulated: where all nodes are honest (static adversaries) with $a=0.75$ and $N=1000000$, where dynamic adversaries performs the attack for a period equal to $400*P_C$ and then start behaving honestly with $a=0.75$ and $N=1000000$ and a variation of the previous scenario with $a=0.75$ and $N=100$. The attack performed is the one introduced in [1], where an offending node cheats when contending for medium access, provoking MAC unfairness and resulting in a DoS attack.

First we consider the case where all nodes are honest with $a=0.75$ and $N=1000000$ (Figure 3). Setting the value of the ageing parameter decreases the influence of past reports on the trust value update process. Furthermore, the normalization parameter is set to an arbitrarily large number (1000000) in order to consider as much past evidence about the nodes as possible (since the simulation considers 1000 periods, all evidence received is effectively considered). The results show that T_{c_i} starts gradually increasing and stabilizes after some periods of oscillation in the beginning of the simulation, showing that the trust between the coordinator and the honest nodes is increasing over time. We note that this results reflect the same behavior of the original model in an static adversary scenario.

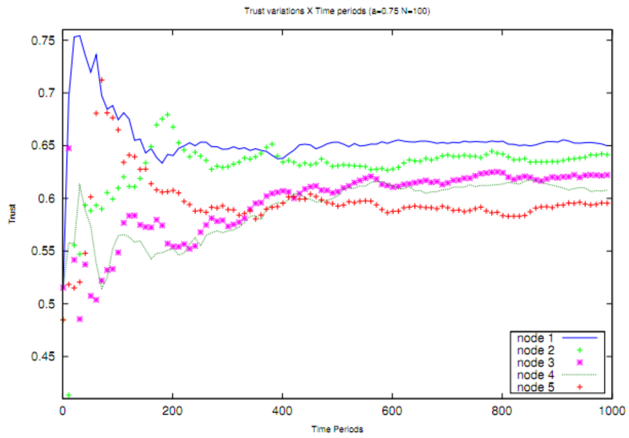


Figure 3: Trust between the PAN Coordinator and the nodes T_{c_i} versus time periods P_C in the case where all nodes are honest with $a = 0.75$ and $N = 1000000$

The case of dynamic adversaries with $a = 0.75$ and $N = 1000000$ is shown in Figure 4. In this scenario we analyse the model's behavior in a realistic dynamic setting, with nodes alternating between honest and malicious behavior in the course of the simulation. While nodes 2,3 and 4 behave honestly during the whole simulation, node 5 performs the attack until period 400 ($time = 400 * P_C$) and then starts behaving honestly. Conversely, node 1 behaves honestly until period 400 ($time = 400 * P_C$) and then starts performing the attack. The parameters are similar to the previous scenario, causing all evidence received to be considered and decreasing the influence of prior information on the trust update process. It is possible to observe how T_{c_5} and T_{c_1} respectively exponentially increase and decrease after a reasonably large period of stabilization. The effect of the previous reputation data collected on the convergence speed after the nodes change their behavior is attenuated by the ageing parameter, enabling faster convergence to the new trust values.

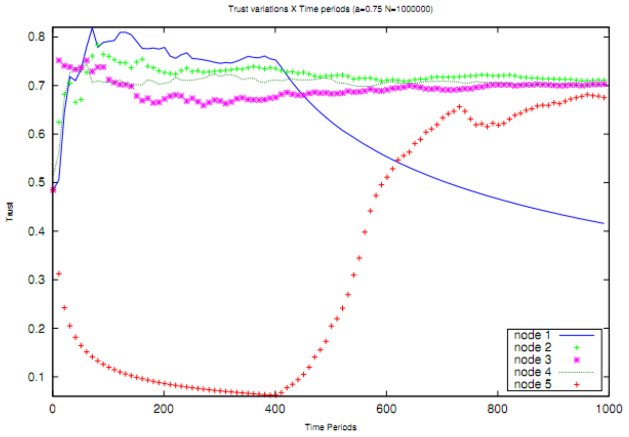


Figure 4: Trust between the PAN coordinator and the nodes T_{c_i} versus time periods P_C in the case of dynamic adversaries that change behavior at period 400 with $a = 0.75$ and $N = 1000000$

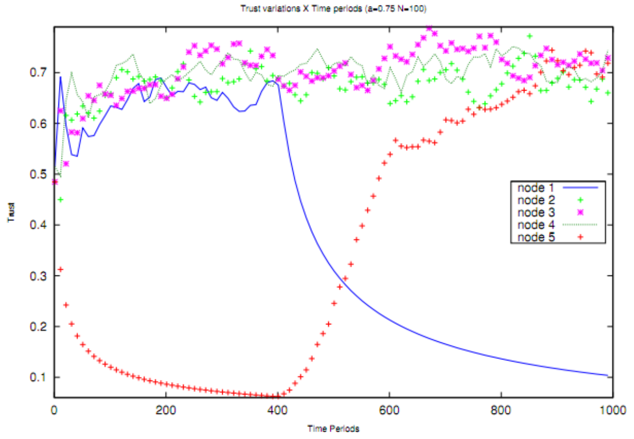


Figure 5: Trust between the PAN coordinator and the nodes T_{c_i} versus time periods P_C in the case of dynamic adversaries that change behavior at period 400 with $a = 0.75$ and $N = 100$

The case of dynamic adversaries with $a = 0.75$ and $N = 100$ is shown in Figure 5. In this scenario we analyse the model's behavior in a realistic dynamic setting, with nodes alternating between honest and malicious behavior in the course of the simulation. While nodes 2,3 and 4 behave honestly during the whole simulation, node 5 performs the attack until period 400 ($time = 400 * P_C$) and then starts behaving honestly. Conversely, node 1 behaves honestly until period 400 ($time = 400 * P_C$) and then starts performing the attack. In this case, the normalization parameter is set to 100, meaning that only the last 100 past reports (i.e. evidence) are considered in the trust update process. It is possible to observe how T_{c_1} exponentially decreases faster than it decreased in the previous scenario, while T_{c_5} increases similarly to the previous scenario but presents a more linear growth. The effect of the previous reputation data collected on the convergence speed after the nodes change their behavior is attenuated by the ageing parameter, enabling faster convergence to the new trust values. Moreover, applying the normalization procedure for evidence samples greater than 100 reports allows the model to analyse only the last 100 reports, capturing the dynamic adversaries' adaptive behavior oscillations and the consequent trust value variations with greater precision.

VI. Conclusion

Wireless sensor networks based on IEEE 802.15.4 are vulnerable to a number of DoS attacks and are subject to MAC unfairness issues. Trust based security solutions for the MAC layer in LR-WPANs and WSNs are a resource efficient countermeasure against attacks based on MAC protocol subversion and unfairness. However, current trust models for the MAC layer of ad-hoc and sensor networks are not effective in dynamic settings, where adversaries adaptively alter their behavior. Furthermore, these trust models are not properly adaptable to different contexts, where it is necessary to control the convergence rate of trust value and the quantity of prior evidence considered in the process of estimating a node's trustworthiness. We propose a novel context-dependent bayesian trust model which is adaptable to different environment through the modification of ageing and normalization parameters, efficiently thwarting attacks based on the MAC layer without overloading node's constrained resources with cryptographic calculations and packet overhead transmission. With this result we solve the open problem stated in [1] of adding a more precise ageing factor and means of controlling the trust models use of prior information to the bayesian communication trust model originally proposed. As a future work this trust model could be generalized and adapted to other protocols and networks, also, an algorithm for intelligent adaptive adjustment of the trust model parameters could be proposed. This trust model could also be adapted to serve as a component for a Cross-Layer trust model, integrating data collected at the MAC and Network layers.

References

[1] Bernardo David and Rafael Sousa. A Bayesian Trust Model for the MAC Layer in IEEE 802.15.4 Networks. *I2TS 2010*, 0.0.

[2] Ganeriwal, Saurabh and Srivastava, Mani B. Reputation-based framework for high integrity sensor networks. *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 66--77, New York, NY, USA, 2004. ACM.

[3] Gill, K. and Shuang-Hua Yang. A scheme for preventing denial of service attacks on wireless sensor networks. *Industrial Electronics, 2009. IECON '09. 35th Annual Conference of IEEE*, pages 2603 -2609, 2009.

[4] IEEE. IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks specific requirements part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs). *IEEE Std 802.15.4-2003*, :1-670, 2003.

[5] Audun Josang and Roslan Ismail. The Beta Reputation System. *In Proceedings of the 15th Bled Electronic Commerce Conference*, 2002.

[6] Karlof, Chris and Sastry, Naveen and Wagner, David. TinySec: a link layer security architecture for wireless sensor networks. *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 162--175, New York, NY, USA, 2004. ACM.

[7] Koksal, Can Emre and Kassab, Hisham and Balakrishnan, Hari. An analysis of short-term fairness in wireless media access protocols (poster session). *SIGMETRICS Perform. Eval. Rev.*, 28(1):118--119, 2000.

[8] Z. Li and S. Nandi and A.K. Gupta. Achieving MAC fairness in wireless ad-hoc networks using adaptive transmission control. *Computers and Communications, IEEE Symposium on*, 1:176-181, 2004.

[9] Momani, M. and Challa, S. and Alhmouz, R. Can we trust trusted nodes in wireless sensor networks?. *Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on*, pages 1227-1232, 2008.

[10] Perrig, Adrian and Stankovic, John and Wagner, David. Security in wireless sensor networks. *Commun. ACM*, 47(6):53--57, 2004.

[11] Adrian Perrig and Robert Szewczyk and Victor Wen and David Culler and J. D. Tygar. SPINS: Security Protocols for Sensor Networks. *Wireless Networks*, pages 189--199, 2001.

[12] A. Rajaram and S. Palaniswami. The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks. *International Journal on Computer Science and Engineering*, 2(2):400 - 408, 2010.

[13] David R. Raymond and Scott F. Midkiff. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Computing*, 7(1):74-81, 2008.

[14] Ries, Sebastian. Extending Bayesian trust models regarding context-dependence and user friendly representation. *SAC '09: Proceedings of the 2009 ACM symposium on Applied Computing*, pages 1294--1301, New York, NY, USA, 2009. ACM.

[15] Anthony D. Wood and John A. Stankovic. Denial of Service in Sensor Networks. *Computer*, 35(10):54-62, 2002.

[16] Zheng, Jianliang and Lee, Myung J. A comprehensive performance study of IEEE 802.15.4. *Sensor Network Operations*, :218--237, 2006.

[17] Jianliang Zheng and Myung J. Lee and Michael Anshel. Toward Secure Low Rate Wireless Personal Area Networks. *IEEE Transactions on Mobile Computing*, 5(10):1361-1373, 2006.

AUTHORS PROFILE

Rafael Timóteo de Sousa Junior recieved his B.E. degree in electrical engineering from the University of Paraíba, Paraíba, Brasil, in 1984, the MSc degree from Ecole Supérieure D'electricité Supelec, France, in 1985 and the PhD degree from Université de Rennes, France, in 1988. His research interests include MANETs, secure routing and computational trust.

Rafael Timóteo de Sousa Junior recieved his B.E. degree in electrical engineering from the Mackenzie University in 1996, the MSc degree from

University of Brasília, Brasília, Brazil, in 2008. He is currently persuing a PhD degree in electrical engineering at the University of Brasília. His research interests include cloud security, online banking and computational trust.

Marcelo Dias Holtz recieved his B.E. degree in network engineering from the University of Brasília, Brasília, Brazil, in 2009. He is now persuing a MSc in electrical engineering at the University of Brasília. His research interests include computational trust, cloud computing and network management and security.

Beatriz Campos Santana recieved her B.E. degree in Information Systems from UNIPLAC, Brasília, Brazil, in 2007. She is now persuing a MSc in electrical engineering at the University of Brasília. Her research interests include computational trust, secure routing and computational trust.

Bernardo Machado David is currently persuing his B.E. degree in network engineering at the University of Brasília, Brasília, Brazil, in 2009.His research interests include cryptography, information theory, MANETs, computational trust and network management and security.