Reputation-based Intrusion Detection System for wireless sensor networks

Keldor Gerrigagoitia*, Roberto Uribeetxeberria†, Urko Zurutuza‡, and Ignacio Arenaza§
Electronics and Computing Department
Faculty of Engineering
Mondragon University
Arrasate-Mondragon, Spain
*Email: keldor.gerrikagoitia@alumni.eps.mondragon.edu
†‡§Email: {ruribeetxeberria,uzurutuza,iarenaza}@mondragon.edu

***Abstract*—Wireless Sensor Networks (WSNs) can be used in a broad range of applications from complex military operations to simple domestic environments. This makes security a vital characteristic in WSNs. There have been numerous studies in the field of security in sensor networks, being Intrusion Detection System (IDS) among the most used tools in this area. This study proposes a new IDS design based on reputation and trust of the different nodes of a network for decision-making and analysis of possible sources of malicious attacks.**

***Index Terms*—Intrusion Detection, Wireless Sensor Network, Reputation, Trust, Security.**

I. Introduction

A WSN [1] is a network compounded by small embedded systems that gather information from its sensor, make a set of computations and communicate via wireless links with other nodes. These nodes can be deployed in many environments and each environment has its own needs. For example, in hostile ones WSN need to be secure and trustworthy, while in unattended environments they need to be autonomous and self-sufficient. Due to these reasons the complexity of sensors may vary significantly, from small computation power with low energy consumption to large nodes with complex systems used in military environments. But in most cases nodes are designed as simple as possible to minimize production costs and reduce power consumption.

Because nodes are often responsible for managing critical systems, security becomes one of the most important features in WSN. In hostile environments an adversary can manage to compromise one or more nodes, and the security systems have to minimize the damage. Prevention methods like encryption and authentication can reduce intrusions but not eliminate them. These methods cannot defend the system from compromised nodes that are already part of the network and thus use proper private keys. Security research assumes that weak links, which can be exploited, can always exist in the network, no matter how many intrusion prevention policies are established. The undetected weak links provide the attackers a point to provoke network failures. If a system is able to detect the intruder soon enough, appropriate measures can be taken before any damage is done or any data is compromised. In this area, intrusion detection systems are responsible for detecting a possible attack and minimizing the risks.

In this work we review the work done so far on Intrusion Detection Systems for WSN, then we focus on reputation and trust based systems, and finally we propose a new architecture based on the most suitable features of the reviewed systems that can lead to a complete and industrially usable IDS for WSN.

II. Related Work

During the last few years, some works have been published where intrusion detection systems were applied in WSN environments [2] [3] [4]. Most of these studies have covered the local detection problem, where nodes detect specific attacks that happen in their network.

A description of the requirements of a WSN oriented IDS is given in [5]. Embedded systems, by definition, must use the minimum resources possible to preserve their lifetime. One of the main characteristic is that it must work with only localized and partial data due to the possible lack of centralized points with a global view. Other characteristics are that the system can never trust any node completely and that the system should be fully distributed. Finally, it should be able to withstand an attack to the IDS itself.

Similar IDS are proposed in [3] and [6], where there are special purpose nodes in the network which are responsible for monitoring other nodes. They listen to messages in their same radio range and store message fields that can be useful to an IDS running in a sensor node. There are some other different points of view in the design of IDS in WSN, for example [7], where nodes are selfish and try to preserve their resources at expense of others. Other works, [8] and [9], keep the idea of no collaboration among sensor nodes and assume that the ad hoc network routing protocols can be applied to WSN.

A distributed intelligent agent-based system is proposed in [10]. It detects intrusions in a fully distributed way. This characteristic comes from the fact that all nodes have an independent IDS agent installed. This agent is able to detect intrusions locally, always based on data collected by the same node and by neighbour nodes. Once an intrusion is detected, the responses or actions taken to isolate it are based on a decision that is made collaboratively by the set of participating nodes. Other collaborative approaches on the local detection of selective forwarding and sinkhole attacks can be found in [11] and [12].

Intrusion detection in ad-hoc networks has had more attention as described in [13]. Distributed and collaborative IDS architectures are preferable for these networks. This way, detailed distributed designs, actual detection techniques and system performance have been more deeply studied. It must be taken into account that wireless sensor networks compared to ad-hoc networks are generally much more resource constrained. Approaches to a more sensor collaborative system rather than a specific attacks detection system can be found in [2].

Regarding distributed systems, LIDeA is a lightweight WSN oriented IDS [14]. It is based on a distributed architecture, where nodes listen to their neighbour nodes and collaborate with each other in order to detect an intrusion successfully. LIDeA, uses components and interfaces of TinyOS [15], a free and open source component-based operating system and WSN oriented platform.

Another distributed IDS is presented in [16]. In this work a misuse-based combined with anomaly-based IDS in a two-level distributed hierarchy is proposed. There are two main parts in this IDS: The IDS Central Agent, which is in charge of recognizing attacks by exploiting control data and alarms sent by Local Agents (LA), and the IDS Local Agent which is located in each node. This LA is compound by other three parts, the Local Packet Monitor (it is in charge of analysing the traffic flowing through the node), the Control Data Collector (gathers measures to be sent to the IDS Central Agent) and the Local Detection Engine (it is in charge of detecting suspicious activities and rising alerts, receiving responses from the Central Agent and performing possible recovery actions). The usage of an anomaly-based approach for local detection might result in a high number of false positives. The usage of temporary local decisions allows the mitigation of such sided effect and especially avoids the triggering of responses for intermittent anomalies. The temporary decisions made by the Local Agent may be made persistent by the Central Agent. The Central Agent detects attacks based on known patterns of attack features (misuse-based detection), and when it makes its final decision, the base station propagates the decision to the Local Agents for its enforcement.

Finally a Hybrid Intrusion Detection System (HIDS) has been proposed in [17]. This system is based on a hybrid star architecture and applied to Cluster Wireless Sensor Networks (CWSN) where intrusions are detected by Cluster Heads. The proposed HIDS consists of an anomaly detection and misuse detection model. It filters a large number of packet records, using the anomaly detection model, and performs a second detection with the misuse detection model, when the packet can be determined as an intrusion. Therefore, it efficiently detects intrusions and avoids the resource waste. Finally, integrates the outputs of the anomaly detection and misuse detection models with a decision making model. This determines the presence of an intrusion, and classifies the type of the attack. The output of the decision making model is then reported to an administrator for follow-up work. This method not only decreases the threat of having successful attacks in the system, but also helps the user handle and correct the system further with hybrid detection.

A similar HIDS is presented in [18], where the system is based in anomaly and misuse techniques. The attacks are detected through the collaboration of global and local agents integrated in the application layer of nodes. A defense method and four algorithms to detect and isolate malicious nodes are also proposed.

III. Reputation and Trust-based Systems in WSN

In recent years a growing number of studies have been conducted on the use of reputation systems in sensor and ad-hoc networks [19]. But only RFSN [20] and DRBTS [21] have focused on the use of reputation systems in WSN.

DRBTS stands for “Distributed Reputation and trust-based Beacon Trust System”. This model makes use of some special nodes called Beacon Nodes (BN) that can monitor each node around and report to the rest of the network of gathered information. This data is gathered using watchdog mechanism, this mechanism is used assiduously in WSNs and is explained in [22].

Meanwhile RFSN or Reputation-based Framework for Sensor Network is a design based on the watchdog mechanism as well, but this design keeps this mechanism in each node of the network. Making use of this, a node can classify each action as a cooperative or non-cooperative creating the reputation of the nodes around.

IV. Architecture of the Proposed IDS

The IDS proposed in this work is a distributed anomaly detection based system, where each node will have an IDS agent that will monitor local activities. If the local agent cannot determine the behaviour of an activity, this agent will contact with the agents near him to determine if that activity is malicious or not. Once that one activity is considered malicious, the IDS will take necessary measures to mitigate the situation.

IDS agents located in nodes are compounded by five parts; Local Data Collection module gathers different inputs, systems logs, network traffic or sensor values. After, recollected inputs are analysed by Local Detection Engine that will raise alarm flag if finds evidence of malicious activities. Once alarm is raised the Local Response and Global Response will take care of the situation to mitigate the failure. But if the Local Detection engine cannot determine the conduct of a behaviour, the Cooperative Detection engine will ask nodes’ opinion about that activity, to define if it is normal or malicious.

The detection system proposed for this IDS is an hybrid between anomaly and specification-based detection systems. At the initialization of the system some specific parameters are configured, as response time or frequency of notifications. This allows the IDS to monitor the different protocols of the system

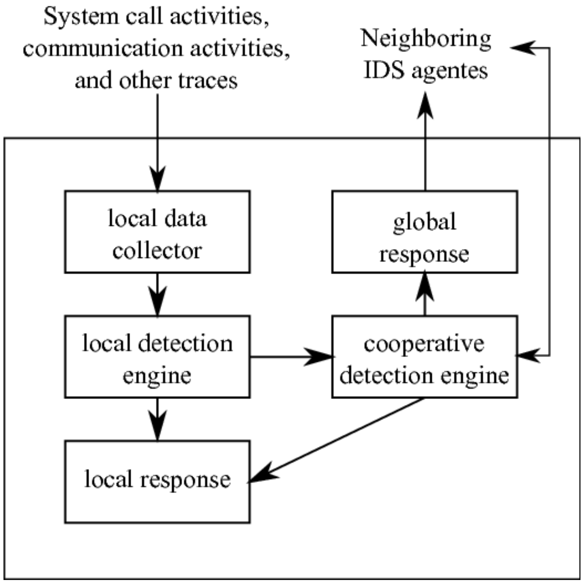

Fig. 1. Local IDS architecture

and search for possible attacks. Besides, the IDS also has a series of rules based on node behaviour to cover the widest range of attacks that would not be covered with specification-based detection.

To determine the behaviour of a node, reputation and trust is used. If node A suspects about the confidence of node B, node A can ask the other nodes their reputation value for node B. The most shared opinion about the confidence of node B can confirm or discard the suspicions of node A.

To determine the reputation of node B, node A takes into account the communications and iterations between them. To calculate the reputation is used Beta distribution [23] [24] which uses correct and incorrect iterations to give a reputation value.

$$R_{ij} = \beta(\alpha_j + 1, \beta_j + 1) \tag{1}$$

where R_{ij} represents the confidence of the node i for node j, α_j are the cooperative iterations and β_j are the no cooperatives ones.

$$T_{ij} = \mathbb{E}(\beta\{\alpha_j + 1, \beta_j + 1\}) = \frac{\alpha_j + 1}{\alpha_j + \beta_j + 2} \tag{2}$$

where T_{ij} is the trust of a node for other node, is given by a value from 0 to 1 (1 meaning absolute trust) and is based on Beta distribution.

On the other hand, if a node has doubts about another node and cannot determine with certainty if it is malicious or not because of lack of data, this node can ask its neighbourhood for information to determine with accuracy the aim of the suspicious node. The neighbourhood of a node is compounded by the nodes that are not farther than two hops.

To calculate the new reputation of a node using the information given by the nodes in the neighbourhood, the same system of second hand information used in [20] and explained in [24] is applied.

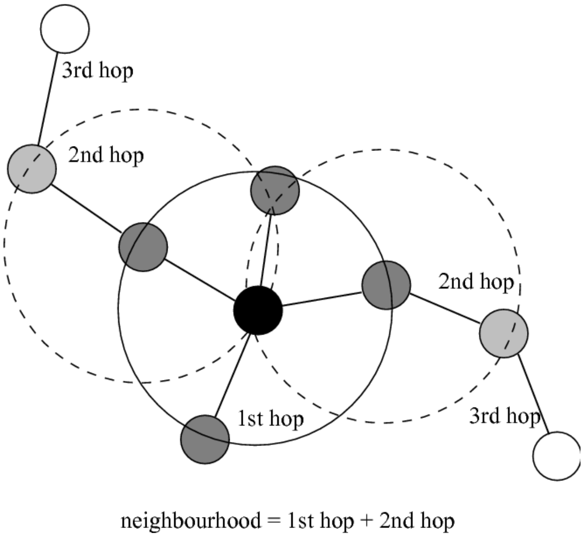

Fig. 2. Node neighbourhood definition

$$\alpha_j^{NEW} = \alpha_j + \frac{\{2 * \alpha_k * \alpha_j^k\}}{\{(\beta_k + 2) * (\alpha_j^k + \beta_j^k + 2)\} + \{2 * \alpha_k\}} \tag{3}$$

$$\beta_j^{NEW} = \beta_j + \frac{\{2 * \alpha_k * \beta_j^k\}}{\{(\beta_k + 2) * (\alpha_j^k + \beta_j^k + 2)\} + \{2 * \alpha_k\}} \tag{4}$$

When a node asks for information about another node to the neighbourhood, it receives observations that nodes of neighbourhood have about the node in question (α_j^k, β_j^k), where α_j^k are the correct iterations performed by node k with node j and β_j^k are the incorrect ones.

With this second hand information a node can calculate the new iteration values that are used to recalculate the reputation. Moreover, information received from nodes with high reputation will have greater weight than those with less reputation.

V. Comparison between proposed IDS and analysed IDS

As shown in table I, we have analysed the characteristics of the more representative IDS with the IDS proposed in this paper.

The first IDS that was analysed was proposed in [16], despite being distributed and to have great strength and great success in attack detection, we find that the centralized architecture used in this proposal has no place in our needs, so we focus on analysing only those IDS that can operate autonomously without a central server that maintains the proper functioning of the network.

The IDS proposed in [3], is a solution based on the classical architecture where information is collected, a set of rules is applied and they confirm the intrusion attempr or not. This

TABLE I
SUMMARY OF REPRESENTATIVE SOLUTIONS AND PROPOSED SOLUTION

Specification		LIDeA	[16]	[10]	[3]	Proposed Solution
Detection System	Anomaly	✓		✓		✓
	Misuse	✓	✓	✓	✓	
	Specification-based					✓
Adaptable	Automatic	✓		✓		✓
	Human Interaction		✓		✓	
Architecture	Centralized		✓			
	Distributed	✓		✓	✓	✓
IDS Location	Each node	✓	✓	✓	✓	✓
	Central		✓			
	Cluster Heads					
Cooperation		✓		✓		✓
Lightweight		✓				✓
Reputation Based						✓

solution even being simple and effective, does not meet our demands, as we consider essential the cooperation between nodes to develop a quality IDS in the field of WSN.

LIDeA and [10] on the other hand are two distributed IDS that base their analyses on cooperation between nodes. They have differences in the mechanisms of detection of anomalies, but overall the biggest difference is that LIDeA is aimed at keeping the network traffic as low as possible without overloading the network channel with IDS messages.

Taking into account our needs and the characteristics of the analysed IDS, our proposed IDS is designed to be adaptable, distributed, cooperative, lightweight and reputation-based.

LIDeA satisfies the vast majority of the main requisites that we see as essential to create an IDS for WSN, but we find it imperative the use of a reputation system for help to differentiate malicious nodes which are not. Although this feature increases the level of complexity and therefore the resource usage of nodes, it also increases the performance of the IDS for detecting attacks.

VI. Conclusion

As discussed in this paper, different versions of IDS have been proposed in recent years with multiple architectures for detecting WSN attacks. In this preliminary work we have considered an IDS based on cooperation between nodes and fully distributed architecture.

Keeping these two main features we have proposed an architecture of cooperation, based on reputation to create a network of autonomous sensors capable of detecting most kind of attacks and network failures using an anomaly detection system together with specification-based detection system. All this designed from the premise of creating a system that fits the characteristics of sensor networks and maintaining the protocol as lightweight as possible to guarantee the autonomy of the nodes.

Acknowledgment

This work was developed within nSHIELD project (http://www.newshield.eu) co-funded by the ARTEMIS JOINT UNDERTAKING (Sub-programme SP6) focused on the research of SPD (Security, Privacy, Dependability) in the context of Embedded Systems.

This work is partially supported by the Embedded Systems Group, supported by the Department of Education, Universities and Research of the Basque Government.

References

[1] C. Townsend and S. Arms, “Wireless sensor networks: Principles and applications,” *Sensor technology handbook*, vol. 11, no. 6, pp. 575–589, 2005.

[2] I. Krontiris, Z. Benenson, T. Giannetsos, F. Freiling, and T. Dimitriou, “Cooperative intrusion detection in wireless sensor networks,” *Wireless Sensor Networks*, pp. 263–278, 2009.

[3] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, “Decentralized intrusion detection in wireless sensor networks,” in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*. ACM, 2005, pp. 16–23.

[4] P. Techateerawat and A. Jennings, “Energy efficiency of intrusion detection systems in wireless sensor networks,” in *Proceedings of the 2006 IEEE/WIC/ACM international conference on Web Intelligence and Intelligent Agent Technology*. IEEE Computer Society, 2006, pp. 227–230.

[5] A. Stetsko, L. Folkman, and V. Matyas, “Neighbor-based intrusion detection for wireless sensor networks,” in *International Conference on Wireless and Mobile Communications*. Los Alamitos, CA, USA: IEEE Computer Society, 2010, pp. 420–425.

[6] I. Onat and A. Miri, “An intrusion detection system for wireless sensor networks,” in *Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob’2005), IEEE International Conference on*, vol. 3. IEEE, 2005, pp. 253–259 Vol. 3.

[7] F. Kargl, A. Klenk, M. Weber, and S. Schlott, “Sensors for detection of misbehaving nodes in manets,” in *Detection of Intrusions and Malware & Vulnerability Assessment, GI SIG SIDAR Workshop, DIMVA*. Citeseer, 2004, pp. 83–97.

[8] L. C. Eik, N. M. Yong, L. Christopher, and P. Marimuthu, “Intrusion detection for routing attacks in sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 2, no. 4, pp. 313–332, 1900.

[9] V. Bhuse and A. Gupta, “Anomaly intrusion detection in wireless sensor networks,” *Journal of High Speed Networks*, vol. 15, no. 1, pp. 33–51, 2006.

[10] A. Giannetsos, “Intrusion detection in wireless sensor networks,” Master’s thesis, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA, 2008.

[11] K. Ioannis, T. Dimitriou, and F. C. Freiling, “Towards intrusion detection in wireless sensor networks,” in *Proceedings of the 13th European Wireless Conference*, 2007.

[12] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, “Intrusion detection of sinkhole attacks in wireless sensor networks,” *Algorithmic Aspects of Wireless Sensor Networks*, pp. 150–161, 2008.

[13] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks,” *Wireless Communications, IEEE*, vol. 11, no. 1, pp. 48–60, 2004.

[14] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Lidea: A distributed lightweight intrusion detection architecture for sensor networks," in *Proceedings of the 4th international conference on Security and privacy in communication netowrks*. ACM, 2008, pp. 1–10.

[15] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, and E. Brewer, "Tinyos: An operating system for sensor networks," *Ambient intelligence*, vol. 35, 2005.

[16] L. Coppolino, S. D'Antonio, L. Romano, and G. Spagnuolo, "An intrusion detection system for critical information infrastructures using wireless sensor network technologies," in *Critical Infrastructure (CRIS), 2010 5th International Conference on*. IEEE, 2010, pp. 1–8.

[17] K. Yan, S. Wang, and C. Liu, "A hybrid intrusion detection system of cluster-based wireless sensor networks," *Proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. 1, pp. 18–20, 2009.

[18] T. H. Hai, F. Khan, and E. N. Huh, "Hybrid intrusion detection system for wireless sensor networks," in *Proceedings of the 2007 international conference on Computational science and Its applications-Volume Part II*. Springer-Verlag, 2007, pp. 383–396.

[19] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and trust-based systems for ad hoc and sensor networks," *Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks*, 2006.

[20] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 3, p. 15, 2008.

[21] A. Srinivasan, J. Teitelbaum, and J. Wu, "Drbts: Distributed reputation-based beacon trust system," in *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*. IEEE, 2006, pp. 277–283.

[22] L. Huang and L. Liu, "Extended watchdog mechanism for wireless sensor networks," *Journal of Information and Computing Science*, vol. 3, no. 1, pp. 39–48, 2008.

[23] S. Buchegger and J. Y. L. Boudec, "A robust reputation system for mobile ad-hoc networks," in *Proceedings of P2PEcon*, 2003.

[24] A. Jsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th Bled Electronic Commerce Conference*, 2002, pp. 41–55.