An Efficient Intrusion Detection System for Selective Forwarding and Clone Attackers in IPv6-based Wireless Sensor Networks under Mobility

Fatma Gara, ENIT, Tunis, Tunisia
Leila Ben Saad, University of Agder, Grimstad, Norway
Rahma Ben Ayed, ENIT, Tunis, Tunisia

ABSTRACT

Security in mobile wireless sensor networks is a big challenge because it adds more complexity to the network in addition to the problems of mobility and the limited sensor node resources. Even with authentication and encryption mechanisms, an attacker can compromise nodes and get all the keying materials. Therefore, an intrusion detection system is necessary to detect and defend against the insider attackers. Currently, there is no intrusion detection system applied to IPv6-based mobile wireless sensor networks. This paper is mainly interested in detecting the selective forwarding and clone attacks because they are considered among the most dangerous attackers. In this work, the authors design, implement, and evaluate a novel intrusion detection system for mobile wireless sensor networks based on IPv6 routing protocol for low power and lossy networks. The new intrusion detection system can be extended to other attacks such as wormhole and sybil attacks. The simulations results show that the detection probability is 100% for selective attackers under some cases.

KEYWORDS


1. INTRODUCTION

Wireless Sensor Networks (WSN) consist of small autonomous and distributed devices that monitor the physical conditions in often hostile and not trustworthy environment. Due to the hostile nature of the deployment environment, security is considered as one of the most challenging issue in WSN. Security is vital for ensuring the integrity, authenticity, and confidentiality of the critical information. Attacks in WSN can include routing attacks, black hole attack, sinkhole attack, wormhole attack, selective forwarding attack and node clone attack (Wang, 2006). Most of works in the literature have studied the problem of security and different types of attacks by considering a static WSN. However, the hypothesis of static sensor nodes in the network is not always the case for all WSN applications. In fact, due to the advancement in robotics and microchips technology, a sensor node may also be mobile such as deployed in healthcare applications (Alemdar, 2010) and intelligent transport systems (Qin, 2010). In these applications, sensors which are placed on patients or vehicles, are mobile and need to transmit the collected data quickly and reliably to the sink. Node mobility introduces additional
complexity to static WSN because it will become more vulnerable for intrusion and eavesdropping. Therefore, it is more challenging to detect attacks in mobile WSN compared to the conventional ones.

Attackers in WSN can be insider or outsider. Outsider attackers are initiated from outside and can be prevented by the use of first defense line of defense mechanisms such as authentication, cryptography and key management (Cho, 2012; Meng, 2016; Khanafer, 2010). Whereas, insider attackers can be a legitimate node that operates differently and hence it can have all the authentication keys. Consequently, there will be a need for a second line of defense in the network provided by an intrusion detection system which provides the information related to type of intrusion, location of intruder and intrusion activity active or passive (Ren, 2010).

In this paper, two attacks in mobile WSNs are studied which are selective forwarding attack and clone attack because they are considered among the most dangerous ones in WSNs (Shama, 2012; Kaur, 2016). In addition to that, a novel Intrusion Detection system for mobile wireless sensor networks is designed, implemented and evaluated.

The standardized IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) which is based on IPv6 is considered as an invaluable element for realizing the vision of Internet of Things. This concept aims to connect all physical objects to the Internet enabling them to exchange data and provide useful services. Although, there exists some works that consider IPv6 based-WSNs, most of them only have tried to detect intruders in static WSNs (Wallgren, 2013; Le, 2016).

To the best of our knowledge, this is the first work that designs an IDS for mobile WSN when the standardized RPL protocol is used. The new designed algorithm for detecting malicious nodes is evaluated in large scale networks.

The contributions of the paper can be summarized as follows:

- The problems of security in mobile WSNs and the need of new security solutions are studied.
- Two main attacks: clone attacks and selective forwarding attack are considered. Then, different security solutions proposed in the literature for these two attacks are reviewed.
- A new IDS for IPv6-based mobile WSN to detect these two attacks by taking the benefit of using the RPL protocol are proposed.
- New approaches are used to detect attacks in the proposed IDS such as using the Expected Transmission count metric as a coefficient in the detection of dynamic threshold for the selective forwarding attacks and using the sequential probability ratio test.
- For the clone attack detection, the minimum time that needs a mobile node to leave the radio range of its preferred parent is also introduced in the algorithm which is a new approach.
- RPL global repair property is used in the final step of neutralization to filter the attacker nodes.
- To show the efficiency of our proposed IDS, extensive simulation results are presented.

The remainder of this paper is organized as follows. In Section 3, related works are presented. In Sections 4 and 5, the proposed IDS including system assumptions, attacks model and proposed algorithms are presented. In Section 6, simulation-based results are presented. Section 7 concludes the paper and presents the future work.

2. BACKGROUND: RPL PROTOCOL OVERVIEW

The IPv6 Routing Protocol for Low power and lossy networks (RPL) is a distance vector routing protocol. It has become a standard for low power networks and lossy networks (LLN) since 2012.
Semantic Integration of Structured and Unstructured Data in Data Warehousing and Knowledge Management Systems
[www.igi-global.com/chapter/semantic-integration-structured-unstructured-data/60057?camid=4v1a](www.igi-global.com/chapter/semantic-integration-structured-unstructured-data/60057?camid=4v1a)

Enhancing the Access to Public Procurement Notices by Promoting Product Scheme Classifications to the Linked Open Data Initiative
Jose María Alvarez Rodríguez, Luis Polo Paredes, Emilio Rubiera Azcona, Alejandro Rodríguez González, José Emilio Labra Gayo and Patricia Ordoñez de Pablos (2013). *Teaching Cases Collection* (pp. 1-27).
[www.igi-global.com/chapter/enhancing-access-public-procurement-notices/77197?camid=4v1a](www.igi-global.com/chapter/enhancing-access-public-procurement-notices/77197?camid=4v1a)