International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

INTRUSION DETECTION AND PREVENTION FOR ZIGBEE BASED HOME AREA NETWORKS IN SMART GRIDS

DR.K.RAKESH, V.VENNELA, T.POOJA, R.MAHESHWARI

[1]Assoaciate Professor, Department Of Electronics And Communication Engineering, Malla Reddy Engineering College For Women, Hyderabad.

[2,3,4]Ug Scholar, Department Of Electronics And Communication Engineering, Malla Reddy Engineering College For Women, Hyderabad

ABSTRACT

In this paper, we present a novel intrusion detection and prevention system for ZigBee-based home area networks in smart grids, HANIDPS. HANIDPS employs a model-based intrusion detection mechanism as well as a machine learning-based intrusion prevention system to protect the network against a wide range of attack types. The detection module extracts network features and analyzes them to decide whether the network is in a normal state. We use smart energy profile 2.0 specification as well as IEEE 802.15.4 standard to precisely characterize the expected normal behavior. A set of defensive actions are defined for the prevention system which are effective in stopping various attack types. HANIDPS uses Q-learning and through interactions with environment learns the best strategy against an attack. Use of model-based approach for intrusion detection and dynamic learning for intrusion prevention, as well as employment of effective mechanisms to stop the attacks, provide a high performance for HANIDPS without the need for prior knowledge of the attacks. Soundness of the proposed method is evaluated through extensive analysis and experiments.

I.INTRODUCTION

FROM the advent of the smart grid concept, security has always been a major concern. The need for developing intrusion detection systems (IDSs) tailored for smart grid subsystems was emphasized in the United States (U.S.) National Institute of Standards and Technology (NIST) guidelines for smart grid cyber security [1]. Home area networks (HANs) are subsystems within the smart grid which provide the communication among the smart meters and home devices. The dominant HAN technology in North America and many other countries is ZigBee. Being located in insecure environment and use of wireless technology make HANs vulnerable to cyber attacks [2], [3]; this necessitates application of appropriate IDSs. At the same time, since HANs are located in areas far from the utility, receiving the IDS alarms and acting upon them introduces a large operational cost and delay in stopping the attacks. In traditional IDSs, once an attack is detected, an alarm is sent to a network operator who is responsible for finding the roots of the attack and triggering response operations varying from remote diagnosis to on-site inspection. Considering the large scale of smart grids, when human response is expected, a small percentage of false alarms results in a high operational cost. Therefore, intrusion prevention mechanisms which not only detect but also stop the attacks are highly preferable. In this work we present a novel intrusion detection and prevention system (IDPS) for ZigBee-based HANs, HANIDPS. We use smart energy profile 2.0 (SEP 2.0) protocol specification [4] as well as IEEE 802.15.4 standard (which defines the physical (PHY) and medium access control (MAC) layers of ZigBee), to define a thorough feature space. HANIDPS employs a model-based detection module and a machine learning-based prevention module which dynamically learns the best strategy against an attacker. Through analysis and experiments we show that HANIDPS is able to detect and stop various attack types with a high performance. The main contributions of this work are: • To the best of our knowledge we are the first who address the problem of automatic intrusion prevention in ZigBee-based HANs. Considering that in HANIDPS the prevention operation is performed automatically, the costs of false positives are low and limited to some network overhead. Also the delay in stopping the attacks is significantly shortened compared to when human intervention is required. This reduces the damages caused by possible attacks. • HANIDPS is a novel algorithm which utilizes a modelbased IDS along with a dynamic machine learning-based prevention technique to detect and prevent intrusions with low false positive rate (FPR) and without prior knowledge of attacks. • We introduce a novel high performance spoofing prevention technique as an important defense mechanism in HANIDPS which enables prevention against a variety of attack types. The algorithm is also effective in securing other static wireless sensor networks. This work is an extension to our previous papers [5]–[7]. In [5], we studied the HAN architecture and IDS requirements for HANs. We compared different intrusion detection methods and suggested application of specification based approach. Accordingly we proposed a specification based IDS for HANs in which the feature space was defined based on the network specifications extracted from the IEEE 802.15.4 standard. In [6] we presented an algorithm for detecting spoofing attacks against static IEEE 802.15.4 networks which works by analyzing the received signal strength (RSS) of network packets. We also introduced an RSS-based spoofing prevention mechanism for ZigBee-based HANs in [7]. This work has several new contributions compared to our previous papers. While [5] only targeted the area of intrusion detection, here we introduce an algorithm which not only is able to detect various attack types but also can automatically stop them. For the detection module we use a model based approach which is a combination of anomaly-based and specification-based IDSs. While in [5] we only used IEEE 802.15.4 standard and common features of wireless networks for defining the feature space, here we also use SEP 2.0 protocol specification. Therefore, the definition of feature space in this work is much more precise compared to [5]. Here, the detection module analyzes 6 features of network traffic, one of them is RSS which is examined using the method we introduced in [6]. In the present work, we define several preventive actions for HANIDPS and design a machine learning based method for choosing the best sequence of actions against an attacker. One of these actions is the spoofing prevention algorithm we introduced in [7]. Therefore, while the methods introduced in [6] and [7] were only designed to detect and stop spoofing attacks, the proposed method in this work is able to detect and stop various attack types without having any previous knowledge about them. The machine learning based prevention method designed in this paper which dynamically learns the best strategy against an attacker is completely new. The rest of this paper is organized as follows. We survey the related work in Section II and provide an overview of HAN security threats in Section III. Architecture and algorithm of HANIDPS is explained in Section IV. Sections V and VI present the theoretical analysis and experimental evaluations of HANIDPS. In Section VII we provide a discussion on performance of HANIDPS against evasion techniques and Section VIII concludes the paper.

II.LITERATURE REVIEW

P. Jokar, H. Nicanfar, and V. C. M. Leung, "Intrusion detection system for home area networks in smart grids," in Proc. 2nd IEEE Int. Conf. Smart Grid Commun., Brussels, Belgium, Oct. 2011, pp. 208–213.

A key feature of the smart grid is the introduction of two-way data communications into the power grid. This brings many security challenges, because of the large-scale, difficult-to-secure environment, complexity of smart grid systems, and resource limitations of the smart grid deployments. In this paper, we focus on security and privacy concerns in the context of the smart grid. Existing security mechanisms developed for traditional information technology systems can be used as a basis for designing security measures for the smart grid. However, new methods that meet the special requirements and characteristics of the smart grid are also required. In spite of the obstacles against developing detailed security solutions for the future smart grid, such as uncertainty of the architecture and lack of practical experiences with security attacks, some research has been performed in this area over the last few years. We survey the existing literature on different security aspects of the smart grid and provide directions for further research.

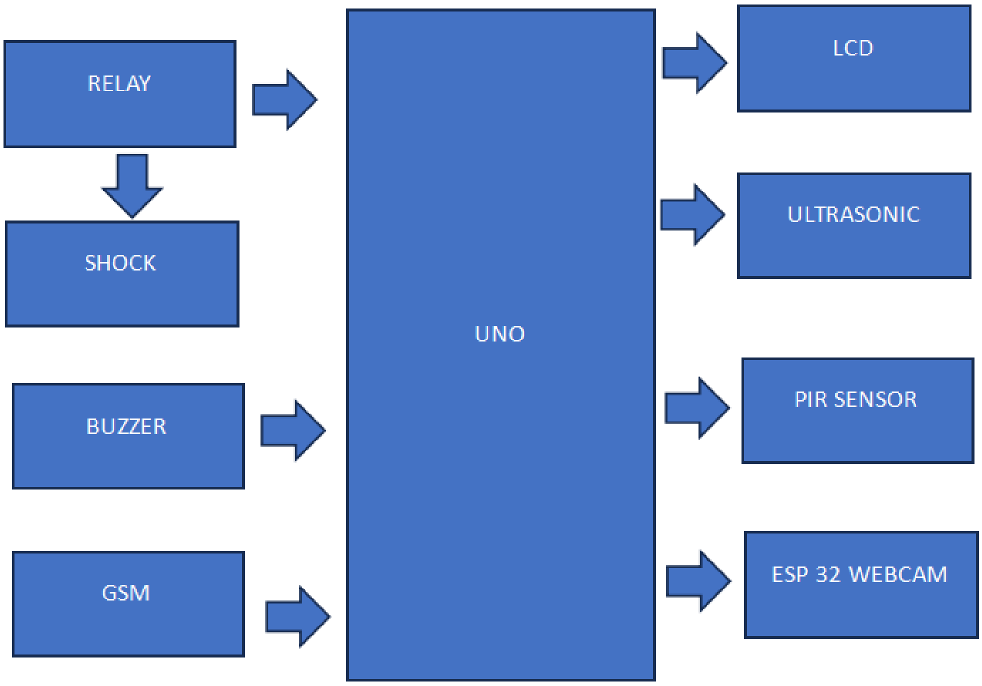
III.EXISTING SYSTEM

Designing IDSs tailored for smart grid subsystems has attracted the attention of researchers over the last few years. Mitchell and Chen [8] introduced a behavior-rule based IDS (BIDS) for securing head ends, distribution access points and smart meters. For each section a set of high-level behavior rules were defined. An intrusion was detected when the behavior rules were violated. This method provides a high accuracy; yet since the behavior rules are high level it is subject to detection delay. Besides, it does not provide an insight into the cause of misbehaviors. A hierarchical distributed IDS for advanced metering infrastructure (AMI) was proposed in

IV.PROPOSED SYSTEM

we present a novel intrusion detection and prevention system (IDPS) for WIFI based HANs, HANIDPS. We use smart energy profile 2.0 (SEP 2.0) protocol specification [4] as well as IEEE 802.15.4 standard (which defines the physical (PHY) and medium access control (MAC) layers of WIFI), to define a thorough feature space. HANIDPS employs a model-based detection module and a machine learning-based prevention module which dynamically learns the best strategy against an attacker.

Block diagram



V.CONCLUSION

In this work we have introduced HANIDPS, a novel IDPS for ZigBee-based HANs. Considering the insecure environment, use of wireless technology and limited resources of HAN devices, HAN is vulnerable to cyber attacks which necessitates application of appropriate IDSs. Also due to the large scale and high cost of false positives, IDPSs which not only detect but also automatically stop the attacks are highly required. HANIDPS combines a model-based intrusion detection method tailored for HAN specifications and a machine learning-based prevention technique which enables dynamic defense against adversaries without prior knowledge of the attacks. Using novel techniques for spoofing prevention, and through utilization of effective mechanism against intentional and unintentional interference, HANIDPS secures the network against a variety of attack types. Extensive analysis and simulations have proved the effectiveness of our approach.

VI.REFERENCES

[1] United States National Institute of Standards and Technology, “Guidelines for smart grid cybersecurity, volume 1—Smart grid cybersecurity strategy, architecture, and high-level requirements,” 2014.

[2] J. Wright. (2010). Smart Meters Have Security Holes. [Online]. Available: http://www.msnbc.com/id/36055667

[3] FBI: Smart Meter Hacks Likely to Spread. Accessed on Apr. 9, 2012. [Online]. Available: http://krebsonsecurity.com/2012/04/ fbi-smart-meter-hacks-likely-to-spread

[4] Sponsored by ZigBee Alliance, “Smart energy profile 2.0 application protocol standard,” ZigBee Public Document 13-0200-00, 2013.

[5] P. Jokar, H. Nicanfar, and V. C. M. Leung, “Intrusion detection system for home area networks in smart grids,” in Proc. 2nd IEEE Int. Conf. Smart Grid Commun., Brussels, Belgium, Oct. 2011, pp. 208–213.

[6] P. Jokar, N. Arianpoo, and V. C. M. Leung, “Spoofing detection in IEEE 802.15.4 networks based on received signal strength,” Ad Hoc Netw., vol. 11, no. 8, pp. 2648–2660, 2013.

[7] P. Jokar, N. Arianpoo, and V. C. M. Leung, “Spoofing prevention using received signal strength for ZigBee-based home area networks,” in Proc. IEEE SmartGridComm, Vancouver, BC, Canada, 2013, pp. 438–443.

[8] R. Mitchell and I.-R. Chen, “Behavior-rule based intrusion detection systems for safety critical smart grid applications,” IEEE Trans. Smart Grid, vol. 4, no. 3, pp. 1254–1263, Sep. 2013.

[9] Y. Zhang, L. Wang, W. Sun, R. C. Green, II, and M. Alam, “Distributed intrusion detection system in a multi-layer network architecture of smart grids,” IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[10] C.-H. Lo and N. Ansari, “CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid,” IEEE Trans. Emerg. Topics Comput., vol. 1, no. 1, pp. 33–44, Jun. 2013.

[11] P.-Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, “Detection of false data injection attacks in smart-grid systems,” IEEE Commun. Mag., vol. 53, no. 2, pp. 206–213, Feb. 2015.

[12] N. Beigi-Mohammadi, J. Misic, H. Khazaei, and V. B. Misic, “An intrusion detection system for smart grid neighborhood area network,” in Proc. ICC, Sydney, NSW, Australia, 2014, pp. 4125–4130.