INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 665-670
RECEIVED : 18/03/2016. PUBLISHED : 25/03/2016
March 25, 2016

ENHANCED SECURITY FRAMEWORK FOR DEFENDING AGAINST UNKOWN ATTACKS ON WSN IN SMART CITIES

M.Naveena[1] ,S.Porchselvi[2] ,R.A.Saranya[3] ,N.Subhashini devi[4] ,S.Gnanavel[5]
Dept of Information and Technology, SKP Engg college, Tiruvannamalai.

Abstract:

In smart cities, wireless sensor networks (WSNs) act as a type of core infrastructure that collects data from the city to implement smart services. The security of WSNs is one of the key issues of smart cities. In resource-restrained WSNs, dynamic ongoing or unknown attacks usually steer clear of isolated defense components. Therefore, to resolve this problem, we propose a hierarchical framework based on chance discovery and usage control (UCON) technologies to improve the security of WSNs while still taking the low-complexity and high security requirements of WSNs into account. The features of continuous decision and dynamic attributes in UCON can address ongoing attacks using advanced persistent threat detection. In addition, we use a dynamic adaptive chance discovery mechanism to detect unknown attacks. To design and implement a system using the mechanism described above, a unified framework is proposed in which low level attack detection with simple rules is performed in sensors, and high level attack detection with complex rules is performed in sinks and at the base station.

Index Terms— Smart city, wireless sensor networks (WSNs), chance discovery, attack detection, software-defined networking

1. INTRODUCTION

Wireless sensor network (WSN) can act as one type of core smart city infrastructure [1]-[4]. Smart grids, smart transportation, smart government and so on can all be realized using WSNs. Moreover, the sensed data can also support additional smart city services. Therefore, the security of WSNs is a key issue for smart cities. Because WSNs are often deployed in potentially adverse or even hostile environments, an attacker can generate all types of threats and attacks [5]-[10]. In addition to traditional threats, there is the possibility for advanced persistent threats, which are sophisticated ongoing and unknown attacks in WSNs [11] [12]. Most existing WSN security components do not include mutable attributes; therefore, traditional security components cannot defend against ongoing attacks with dynamically changing features. In addition, in typical intrusion detection or prevention systems, unknown attacks are regarded as novel attacks because they always contain novel characteristics, which differ from those of traditional attacks. Because most existing intrusion or attack prevention systems in WSNs are built using training samples of known threats, they cannot defend against unknown attacks that can compromise the WSNs. In short, the advanced persistent threats formed by ongoing and unknown attacks can break into WSNs and disrupt their normal tasks. Hence, it is critical to propose an attack prevention scheme that can enhance security for WSNs. There are security mechanisms already in use in some existing applications such as VoIP enterprise environments, trust management, web services, and so on that were developed to address various types of attacks including ongoing and unknown attacks [13]-[15]. However, these schemes cannot be used directly in WSNs. attack detection and access control. Moreover, unlike traditional prevention methods in WSNs [5] [6], the proposed framework employs usage control (UCON) with continuous decision making and dynamic attributes. These two features are helpful in defending against ongoing threats. In addition—and also different from most existing detection methods [6]-[10]—we consider a hierarchical attack detection scheme based on chance discovery, which can update dynamically to defend against unknown attacks. Finally, software-defined networking (SDN) and network function virtualization (NFV) are used to perform attack mitigations.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 665-670
RECEIVED : 18/03/2016. PUBLISHED : 25/03/2016
March 25, 2016

2. PRELIMINARIES

The three-layer network architectures generally used for WSNs [16] [17] include a base station (BS), sink and sensors. There are two main methods for performing data storage in WSNs: distributed methods and centralized methods [18]. The distributed method stores sensed data locally in the sensors, while the centralized scheme sends sensed data from the sensors to the sink.When users access a WSN, the access point (AP) can be at the BS, at a sink, or at a sensor. Because WSNs are usually deployed in unprotected environments, having a robust security scheme for WSNs is imperative for preventing or defending against attacks, especially ongoing and unknown attacks [11] [12].Chance discovery theory [19], proposed by Yukio Ohsawa et. al., is intended to use chance discovery to detect attacks. In chance discovery theory, a chance can be regarded as any event or situation that has a significant impact on decision making. This theory goes beyond the area of data mining; the purpose of chance discovery is to understand the meaning of rare events to help users make decisions to protect the system from risksThere are some existing algorithms for realizing chance discovery.

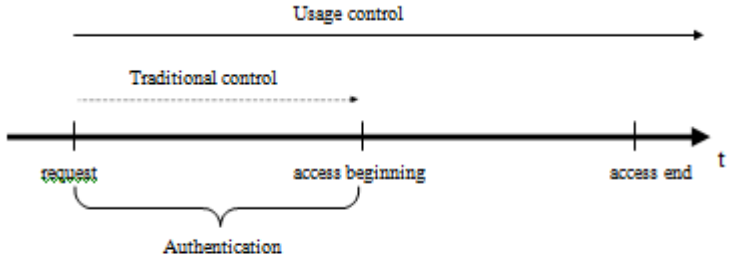

Fig. 1. Usage control

Fig.1. Software-Defined Networking and Network Function Virtualization Technologies

The KeyGraph algorithm [20], proposed by Yukio Ohsawa et. al., is a typical method for implementing chance discovery. KeyGraph extracts key points from the data and then maps the relations among those points as an intuitionistic graph. The lines between the nodes in KeyGraph denote relationships among the data and can then quantify the amount of "tightness" between the objects. In contrast to normal access control methods, UCON performs data control not only at the time of access but also during and after use [21]. Continuous decisions with regard to data access can be made before the access is allowed, during a user's session, or even (via an event) after the session ends. Additionally, its attributes can be updated before access is granted, during use, or after usage has been authorized. Through this type of continuous control, the security level can be substantially improved. Many additional security capabilities, such as data rights management (DRM), can also be performed. A visual depiction of usage control is shown in Fig. 1. The dynamic attribute is on of the most important issues of UCON.

3. BASIC IDEAS BEHIND THE PROPOSED FRAMEWORK

High level attack detection requires relatively complex rules based on data crystallization and can modify those rules adaptively based on the threat situation. In contrast, the rules of low level attack detection using KeyGraph are relatively simple, and the rules are not updated adaptively. A sensor will report unrecognized features to the sink if any unknown events or attacks occur at the sensor.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 665-670
RECEIVED : 18/03/2016. PUBLISHED : 25/03/2016
March 25, 2016

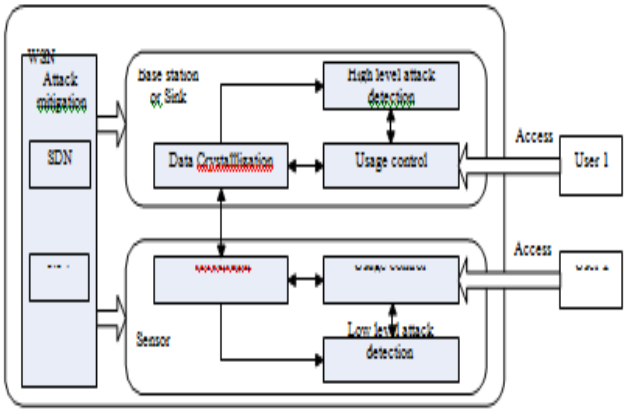

Fig.2. The proposed hierarchical security framework

Based on the high level rules, the sink or the base station will then determine whether the events stem from an attacker or a normal user. The sink or base station can change the rules if necessary according to the novel attack features and return a decision if the attack cannot be identified based on current rules. In addition, attack mitigations for sensors, sinks and the base station are performed based on SDN and NFV. A line directed in the opposite direction cannot be added into G* because G* is a directed graph. In KeyGraph, a connected sub-graph denotes a completed process of rule construction, called a cluster or a foundation. Regarding the hierarchical structure of G*, for the senior node, the layer can be computed as the layer of its junior plus one.

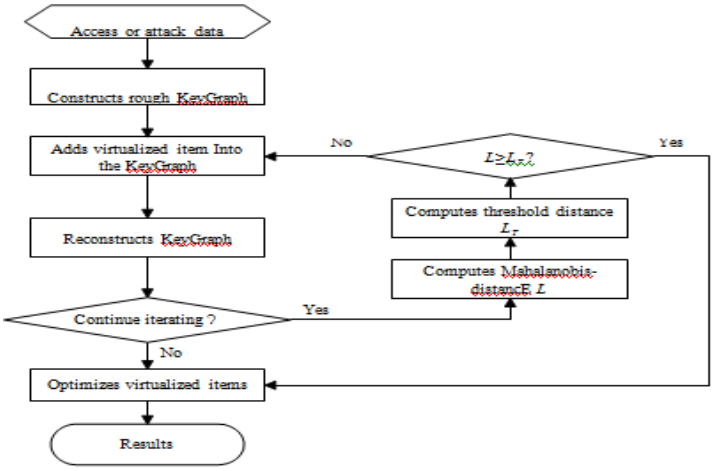

Fig.3. The process of data crystallization based attack detection.

4. ATTACK MITIGATION MECHANISM

Using this mechanism, an SDN controller collects topology and vulnerability information instantly. The information mainly includes network nodes, connectivity and vulnerabilities that lie in the network nodes. It is easy for the SDN-MN controller to do this job because of its central control role in the network. in the network and send them to the SDN controller. Then, the SDN controller measures the current security level driven by this evidence using the algorithms of evidence-driven security assessment discussed in a later section. Using this procedure, an attack graph with new probabilities is

generated that can denote the current security level of the network. Based on the attack graph driven by evidence as mentioned earlier,

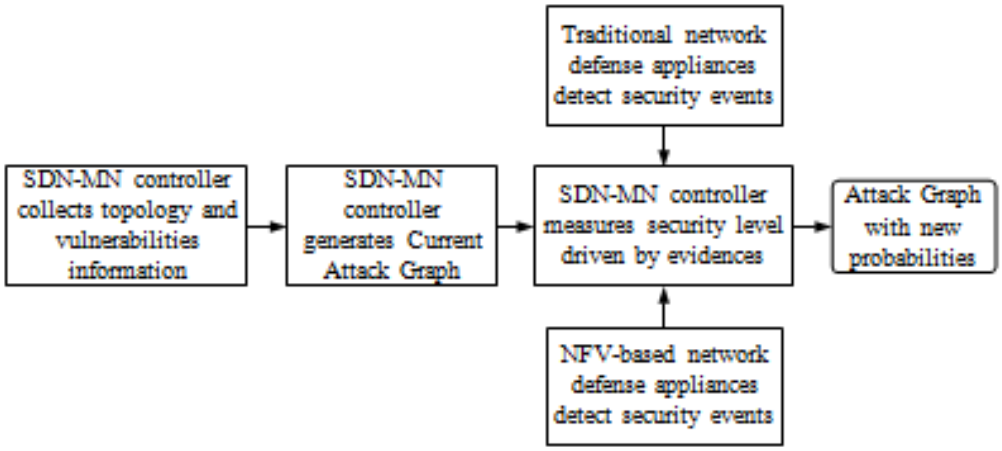

Fig.4. Evidence-driven security assessment using SDN-MN factors andNFV-based detection.

the SDN controller inspects all the VNFs that have already been registered and determines an attack mitigation plan for the current situation that obeys a pre-defined security policy. The algorithms that determine the attack mitigation plan are discussed later. To set up the feature data set for attack detection, we combined UCON and Wi-Fi wireless traffic features [30]. First, some important features of UCON are selected based on the feature selection method in [31]. Second, the MAC header field is extracted as the Wi-Fi standard [30]. To determine the relevance of each feature, Information Gain Ratio (IGR) [32] is used as a measure

5. RESULT ANALYSIS

In WSNs, the sink and base station usually have powerful resources, but resources at the sensors are limited. Therefore, the resource consumption of the proposed scheme (time and memory) in sensors is very important. To perform the evaluation, our scheme was implemented based on TinyOS. We tested it by deploying Tossim. Please note that Tossim simulates MicaZ. The time overhead required by our scheme is shown in Fig. 8. The time overhead is the average time span between the time a sensor receives a request and when it makes a local detection decision.

The time overhead of the methods used in [6] and [11] were tested for comparison. the vertical coordinates denote the time overhead required for detection. The four groups of columns denote four cases that correspond to four types of attacks including APR replay, forgery, Denial of Service (DoS) and ongoing dictionary attacks. For APR replay, forgery, and DoS attacks, 300 items from a training data set and 300 items from the test data set were used to evaluate each attack. However, the ongoing dictionary attack type was not in the training set, and only 300 items of test data were available; therefore, this can be regarded as a type of attack with ongoing and unknown features By using the discrete event system specification (DEVS) Formalism [35], an attack detection simulation was performed to serve as a platform for evaluation.

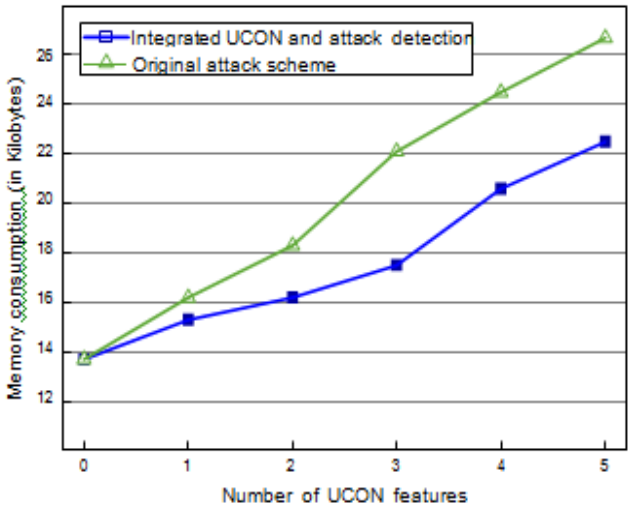

Fig.5. Memory consumption.

The chance discovery was constructed based on the training data set containing the four types of attacks previously described. The detection rate of our scheme as well as detection rates for the schemes.

CONCLUSION

For WSNs in smart cities, ongoing attacks with mutable attributes and unknown attacks with novel features are sophisticated persistent threats that disturb the normal functions of WSNs. In this paper, we propose a hierarchical framework using UCON and chance discovery, which has low-complexity for resource-restrained sensors and high-complexity for sinks or the base station. In this framework, usage control (UCON), which is capable of continuous decision making, is used to address the ongoing attacks. On the other hand, to defend against unknown attacks, we develop an adaptive chance discovery mechanism for attack detection. Moreover, we use SDN and NFV to perform the attack mitigation. The results of the attack experiment and simulations show that our scheme is both feasible for WSNs and offers a significant improvement over current attack detection accuracy.

REFERENCES

[1] S. Chang, Y. Qi, H. Zhu, M. Dong, and K. Ota, "Maelstrom: Receiver-Location Preserving in Wireless Sensor Networks," in Proc. of The 6th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2011), Chendu, China, 2011.

[2] H. Lee, K. Shin, D. H. Lee, "PACPs: Practical Access Control Protocols for Wireless Sensor Networks," IEEE Transactions on Consumer Electronics, vol. 58, no. 2, pp. 491-499, 2012.

[3] M. Abdelhakim, L. E. Lightfoot, J. Ren, and T. Li, " Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 4, pp. 950-959 , 2014.

[4] K. Q. Yan, S. C. Wang, C. W. Liu, "A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks," in Proc. International MultiConference of Engineers and Computer Scientists (IMECS 2009), Hong Kong, China, 2009.

[5] H. Y Lee, T. H. Cho, "A Scheme for Adaptively Countering Application Layer Security Attacks in Wireless Sensor Networks," IEICE Transactions on Communications, vol. E93-B, no. 7, pp. 1881-1889, 2010.

[6] B. P. Zeigler, T. G. Kim, H. Praehofer, Theory of Modeling and Simulation: Integrating Discrete event and Continuous Complex Dynamic Systems. San Diego: Academic Press,

[7] R. Jain and S. Paul, "Network Virtualization and Software Defined Networking for Cloud Computing: A Survey," IEEE Commun. Magazine, vol. 51, no. 11, pp. 24-31, Nov. 2013