This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2517321, IEEE Access

A Hierarchical Security Framework for Defending against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities

Jun Wu, Kaoru Ota, Mianxiong Dong and Chunxiao Li

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. Moreover, software-defined networking (SDN) and network function virtualization (NFV) technologies are used to perform attack mitigation when either low level or high level attacks are detected. An experiment was performed to acquire an attack data set for evaluation. Then, a simulation was created to evaluate the resource consumption and attack detection rate. The results demonstrate the feasibility and efficiency of the proposed scheme.

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

I. Introduction

A 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.

Currently, two complementary types of defense approaches exist to protect WSNs: detection-based approaches, such as intrusion detection (ID), and prevention-based method, such as access control. Although many security schemes have been proposed to address intrusion detection and access control for WSNs [5]-[10], these two types of approaches have traditionally been studied separately. To improve the security of WSNs, we propose a security framework in this paper that combines

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61401273, 61431008. Additionally, this work was supported in part by the JSPS KAKENHI Grant No. 15K15976, 26730056 and the JSPS A3 Foresight Program.

Jun Wu is with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China.

Kaoru Ota and Mianxiong Dong are with the Department of Information and Electric Engineering, Muroran Institute of Technology, Muroran050-8585, Japan (Corresponding author: Kaoru Ota, e-mail: ota@csse.muroran-it.ac.jp).

Chunxiao Li is with the School of Information Engineering, Yangzhou University, Yangzhou, China.

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.

The rest of the paper is organized as follows. Sect. II describes the network architecture and preliminaries. Sect. III explains the basic ideas behind the hierarchical security framework. Sect. IV presents the design principles of the proposed attack detection mechanism. Sect. V describes the attack mitigation mechanism. Sect. VI describes the experiment to acquire the attack data set. Sect. VII describes the evaluation. Finally, Sect. VIII concludes this paper.

II. Preliminaries

A. Access decision-making Architecture

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].

B. Chance Discovery Theory

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 risks.

There are some existing algorithms for realizing chance discovery. 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.

C. Usage Control

The next-generation access control model, usage control (UCON), is a new type of prevention technology. 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.

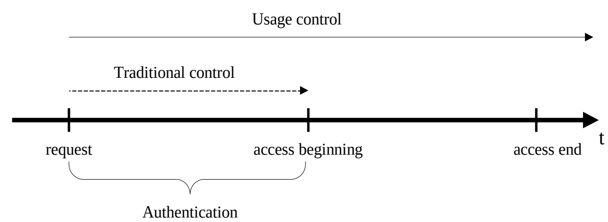


Fig. 1. Usage control.

D. Software-Defined Networking and Network Function Virtualization Technologies

Software-defined networking (SDN) is a novel technology intended to provide network operators with more flexibility in programming their networks, and there are few in the networking community who have escaped its impact [22]-[25]. Network function virtualization (NFV) is another new technology that aids in performing network management effectively. NFV enables network devices to be deployed as virtualized components via software.

E. Sophisticated Attacks

In this paper, we consider two types of sophisticated attacks on defense systems in WSNs, both of which can form advanced persistent threats.

Dynamic ongoing attacks: These attacks usually have dynamically changing features (i.e., wireless MAC address) and can steer clear of the traditional defense components in WSNs because mutable attributes have not been considered in traditional defense components.

Unknown attacks: For intrusion detection or prevention systems, unknown attacks can be regarded as novel attacks. Unknown attacks have quite different characteristics compared with typical attacks. Because most existing intrusion detection or prevention systems in WSNs are designed based on existing rule sets drawn from previous attacks, the systems cannot detect unknown attacks based on their existing rules.

III. Basic Ideas Behind The Proposed Framework

The system model for the proposed hierarchical security framework is shown in Fig. 2. In the proposed framework, each node of a sensor network can perform UCON and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2517321, IEEE Access

chance discovery. The rules for these two modules are stored in a combined rule set. Because the resources of sensors are limited but the sinks and base station have rich computational resources and constant communication capabilities [5], we define two levels of attack detection: (1) low level attack detection in sensors, and (2) high level attack detection in sinks and the base station.

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. 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.

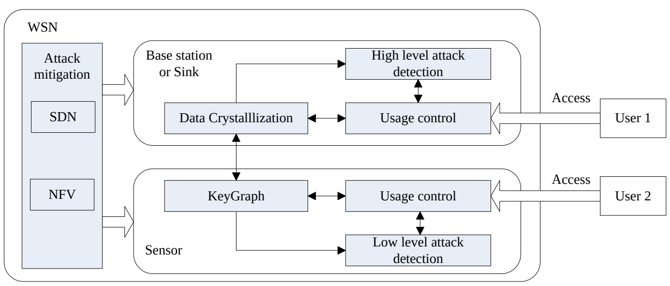


Fig. 2. The proposed hierarchical security framework.

IV. The Proposed Attack Detection Mechanism

A. Reference Monitor Process of UCON

A reference monitor (RM) is one of the most critical issues when applying UCON for access enforcement. ISO/IEC 10181-3 standard [26] has been proposed by the International Organization for Standardization (ISO), which provides a framework for reference monitor access control. Although the standard documentation (ISO/IEC101181-3) for a usage control process explains the system's basic behaviors, it lacks structure. To enhance the usage control model, Statechart is used to model UCON as a reactive system. The details are shown in Fig. 3.

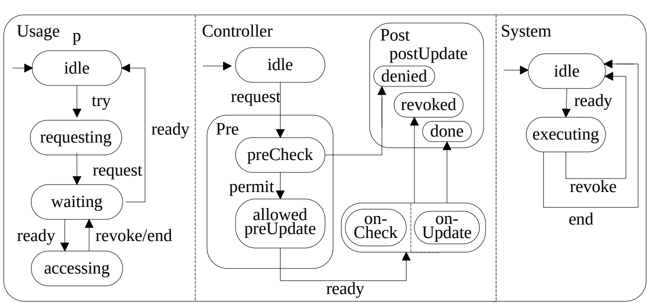


Fig. 3. The core UCON process.

In the usage control process, generating the *try* event causes a usage process p to be initiated. At the start, any required activities to begin the usage process are performed in the *requesting* state. At the same time, the system generates the *request* event. After the *request* event is called, based on the access control policy, a *preCheck* state will be initiated by the usage process p. Access control decisions are determined at that point. When access is denied, the controller launches any defined *postUpdate* activities. When access is granted, the controller launches any defined *preUpdate* activities. Meanwhile, the *ready* event will be generated.

B. KeyGraph based Low Level Attack Detection in Sensors

There are several methods to realize chance discovery. KeyGraph can extract key points of the data and map the relations among them as an intuitionistic graph. The lines between nodes in KeyGraph denote the relations among the data and quantify the degree of tightness between the objects. In this paper, we use KeyGraph to perform chance discovery. First, assume that the original data set of access features S consists of a sequence of sets, denoted as s_1, s_2, …,s_m, …, s_n, where each set s_m is a KeyGraph G_m. Regarding time continuity, an access time is divided into n parts, and each access decision must be provided and selected on time. The graph G_m denotes the access process from time t_m to t_{m+1}, where each vertex of the graph is a feature data set of the access characteristics, and each edge is a relation between two features. The iterations of chance discovery can be performed as follows.

Computation of Connection Values of KeyGraph

Vertexes in G can be sorted according to the frequencies of the vertexes of the outer-edges in G. The association of vertexes in G*, N_i and N_j in G*, can be defined as

$$Connection(N_i, N_j) = \sum_{s_m \in D} \left| N_i, N_j \right|_{G_m} \qquad (1)$$

where N_i and N_j are vertexes of G_m and $\left| N_i, N_j \right|$ means the time interval of a directed line from N_i to N_j present in graph G_m, which corresponds to the feature S_m. Here, the connection value can acts as an assessment of the tightness between N_i and N_j. Pairs of vertexes in G* are identified and sorted based on the connection values between them, which can positively identify the relationship and tightness of a pair of vertexes. 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.

Computation of Tightness

Security nodes in G* are presented as vertexes that connect directly to the high-frequency terms of the cluster or foundation. Here, the tightness of node N is defined as:

$$SecServN(N) = 1 - \prod_{g \subset G^*} \left(1 - KeyG(N, g) / AdjacServ(g)\right) \qquad (2)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2517321, IEEE Access

where g is a foundation, and

$$KeyG(N,g) = \sum_{s_m \in D} W_{G_m}(N,g) \tag{3}$$

$$AdjacServ(g) = \sum_{s_m \in D} \sum_{N \in G_m} W_{G_m}(N,g) \tag{4}$$

$$W_{G_m}(N,g) = \left|NN_g\right|_{G_m} \times Layer(N_g)_{N_g \in g} \tag{5}$$

where the layer value of vertex N_g is denoted as $Layer$ (N_g). The key values are calculated for all the vertexes in G_m, and the nodes with the top security factors will be added if they are not in G*.

KeyGraph iteration is performed using the principles stated above.

Detection Rule Construction

In G*, $W(N$, G*) is the value that denotes feature N connected to the key links around it. The feature nodes with values beyond a reasonable threshold are treated as detection rules that must be satisfied for attack detection; thus, a detection rule can be constructed.

C. Data Crystallization based High Level Attack Detection in BS and Sink

KeyGraph is proposed for a given access data set, which is usually used to find the underlying relations in the data set. In other word, KeyGraph can find important chances with a low frequency of occurrence. However, KeyGraph can only address known features of a data set; it cannot address unknown data sets. In fact, when an unknown attack presents itself, KeyGraph based intrusion detection alone cannot detect it accurately. However, a data crystallization algorithm can address the problem of unknown data and make accurate decisions. Using this method, unknown data can be detected based on the analysis of known data. Here, we use data crystallization [27] to perform high level intrusion detection, in particular, for detecting unknown attacks.

In this high level intrusion detection scheme, KeyGraph is still used for computing the unknown data set. A rough KeyGraph can be obtained, and the "virtualized item" that is related to the unknown data can be added into KeyGraph as a vertex. Next, the relationships between this "virtualized item" and existing vertexes can be established. In other words, by inserting unknown data into the known data, their relationships can be obtained. Isolated vertexes from the KeyGraph can be connected in the KeyGraph by inserting them iteratively as "virtualized items."

For normal access, assume that μ is the mean of the leaf node features vector, and S is the covariance matrix of the same feature vector. Additionally, for the current KeyGraph, assume that θ is a matrix of the feature data of a novel attack. Assume that the covariance matrix of the same feature vector is denoted as H.

Next, based on the calculation of the Mahalanobis-distance, virtual items should be added into the original data set. The Mahalanobis-distance can be calculated based on the following formula:

$$d_M = \sqrt{(\theta-\mu)^T \cdot H^{-1} \cdot (\theta-\mu)} \tag{6}$$

where the minimum Mahalanobis-distance is the threshold L_T, which is the distance from the usual known attack vertex to the normal access central vertex.

After adding the virtual items, the KeyGraph can be reconstructed. When the iteration is finished, the added items should be confirmed by the existing attack data set, which can optimize the KeyGraph. Using this process, the virtual item will be removed if it cannot match the existing attack data set. Finally, based on the final KeyGraph, the results can be obtained.

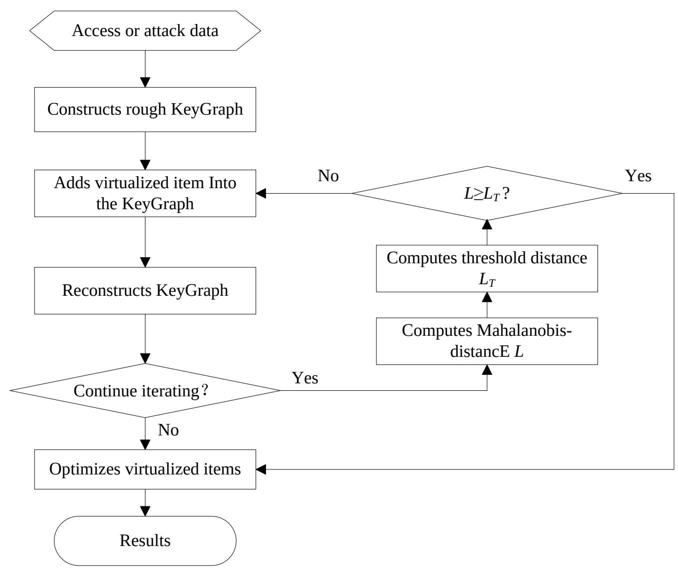


Fig. 4. The process of data crystallization based attack detection.

V. ATTACK MITIGATION MECHANISM

A. Evidence-Driven Security Assessment using SDN-MN Factors and NFV-based Detection

The mechanism of evidence-driven security assessment using SDN factors and NFV-based detection is illustrated in Fig. 3.

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.

Then, the SDN controller generates an attack graph with the current probabilities.

Traditional network defense appliances and NFV-based network defense appliances detect real-time security events

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2517321, IEEE Access

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.

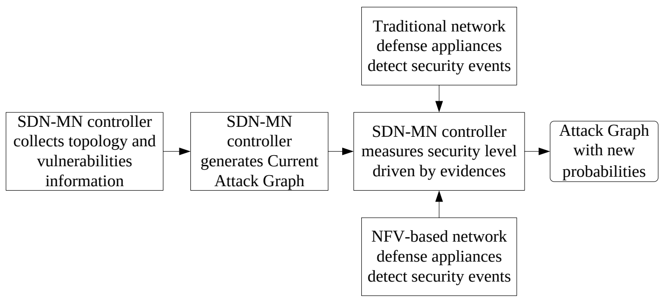


Fig. 5. Evidence-driven security assessment using SDN-MN factors and NFV-based detection.

B. *Proposed Attack Graph*

In a later section, we use the attack graph as a method to measure the static network security level, defined as follows:

Definition 1: A network attack graph is a 7-tuple directed acyclic graph $AG = (S, S_0, G, A, E, \Delta, \Phi)$, where:

- A finite set of state nodes is denoted as $S=\{s_i|i=1,\ldots,N_s\}$.
- A set of the state the attacker wishes to take over is denoted as $S_0 \subseteq S$.
- The purpose of the attack is denoted as $G \subseteq S$.
- A finite set of actions is denoted as $A=\{a_i|i=1,\ldots,N_a\}$.
- A finite set of edges is denoted as $E=(E_1 \cup E_2)$. $\mathrm{Pre}(n)$ and $\mathrm{Con}(n)$ denote the prerequisite nodes and the consequent nodes, respectively.
- A local conditional probability distribution that provides an estimate of whether a given action will be conducted is denoted as $\Delta=\{\delta:(\mathrm{Pre}(a_i), a_i)\rightarrow[0, 1]\}$.
- A local conditional probability distribution that provides an estimate of whether an access is legal can be used, denoted as $\Phi=\{\emptyset:(a_i, \mathrm{Con}(a_i))\rightarrow[0, 1]\}$.

Figure 6 shows a typical attack graph for WSNs.

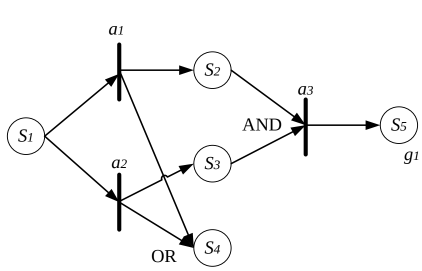


Fig. 6. A typical network attack graph.

1) *Local Conditional Probability Distribution of State Node*

A local conditional probability distribution function of s_i, which is mathematically equivalent to $\Pr(s_i | \mathrm{Pre}(s_i))$, is defined as follows:

1. for AND decomposition:

$$\Pr(s_i | \mathrm{Pre}(s_i)) = \Pr(\cap a_j) \tag{7}$$

where $a_j=\mathrm{Pre}(s_i)$, and

2. for OR decomposition:

$$\mathrm{Pre}(s_i)) = \Pr(\cup a_j) \tag{8}$$

where $a_j=\mathrm{Pre}(s_i)$.

2) *Local Conditional Probability Distribution of the Action Node*

In mathematics, a local conditional probability distribution function of a_i that is equivalent to $\Pr(a_i | \mathrm{Pre}(a_i))$ can be defined as shown in the following formulas:

1. for AND decomposition

$$\Pr(a_i | \mathrm{Pre}(a_i)) = \Pr(\cap s_j) \tag{9}$$

where $s_j=\mathrm{Pre}(a_i)$, and

2. for OR decomposition

$$\Pr(a_i | \mathrm{Pre}(a_i)) = \Pr(\cup s_j) \tag{10}$$

where $s_j=\mathrm{Pre}(a_i)$.

C. *Mechanism of Attack Mitigation using SDN and NFV*

The mechanism of attack mitigation using SDN control and NFV deployment is illustrated in Fig. 7.

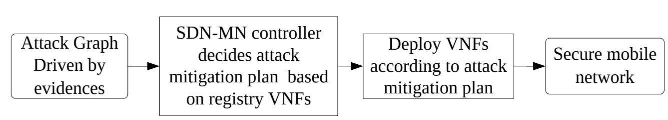


Fig. 7. Mechanism of attack mitigation using SDN-MN control and NFV

Based on the attack graph driven by evidence as mentioned earlier, 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.

The SDN controller obtains the attack mitigation plan and installs the VNF instances into the selected network nodes. VNFs can be deployed as binary compiled code or as interpreted language scripts.

When these steps are complete, the mobile network can defend against the threat and attain a secure status.

D. Attack Mitigation Scheme

Definition 2: Let $m_i(p_i, cost_i)$ be an attack mitigation control for action a_i and p_i be a factor that decreases the probability of the success of a_i. Here, $cost_i$ is the resource cost of deploying the attack mitigation control. Then,

$$\Pr(a_j \mid m_i) = \Pr(a_j) \times p_i \tag{11}$$

In our paper, the goal of an attack mitigation plan is to deploy sufficient attack mitigation controls so that all the probabilities of reaching a target in the attack graph are below a certain threshold and at the same time, to hold the cost for deploying the attack mitigation controls to the minimum value in all mitigation plans.

Definition 3: Let $M = \{m_i | i = 1, \ldots, N_a\}$ be the attack mitigation controls for the actions $A = \{a_i | i = 1, \ldots, N_a\}$. A Boolean vector $T = \{t_i | i = 1, \ldots, N_a\}$ is used to present the attack mitigation plan, where $t_i = True$ means that m_i is adopted in the plan, and $t_i = False$ means that m_i is not adopted in the plan.

Suppose there are p paths for a target in the attack graph, and T is the attack mitigation plan. The maximum value allowed after performing the attack mitigation plan is $Threshold$. Then, the probability of a successful attack for the ith path is $P_i(T)$, and the total cost for the attack mitigation plan T is Cost(T).

To reach the goals of an attack mitigation plan, the values must obey the policy

$$P_i(T) \leq Threshold, \quad i=1,\ldots,p \tag{12}$$

This is equal to

$$G_i(T) = P_i(T) - Threshold \leq 0, \quad i=1,\ldots,p \tag{13}$$

And the following formula can be calculated:

$$\text{minimize } Cost(T) \tag{14}$$

VI. Attack Experiment

To obtain the data set for evaluation, an attack experiment was performed. The WSNs are connected through Wi-Fi for the experiment because many existing real-world WSNs use Wi-Fi technologies [28]. The membership-based metered payment policy [29] is used as a case policy for the experiment.

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. The features of UCON are shown in Table I, and the features of Wi-Fi traffic are shown in Table II.

TABLE I
FEATURES OF WIRELESS TRAFFIC

Features	Description
ResultLogin	Decision before data usage.
DecisOngoing	Decision results during data usage.
Oper Num	Number of operations on rule file.
UCONNum	Number of data usages.
DecisPost	UCON's decision after data usage.

TABLE II
FEATURES OF WIRELESS TRAFFIC

Features	Description
ResultWep	Check the result of ICV of Wired Equivalent Privacy.
Duration	The time the medium is expected to be busy.
Frag More	Whether the frame is a last fragment.
Addr Desti	MAC address of the receiver.
Type Fram	Frame type.
IfRetransmit	Whether the frame is a retransmitted frame or not.
AddrSour	MAC address of the sender.

WSNs were deployed over three wireless stations for this experiment. One station functioned as a server node. Another station was used to generate normal and attack traffic. The last machine was deployed to monitor and record both normal and attack traffic. Attacks were generated based on Backtrack [34].

VII. Evaluation

A. Resource Consumption

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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2517321, IEEE Access

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. In Fig. 7, 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. As shown in Fig. 8, the time overhead required by our scheme is much lower than that of the schemes in [6] and [11], especially for the ongoing dictionary attack.

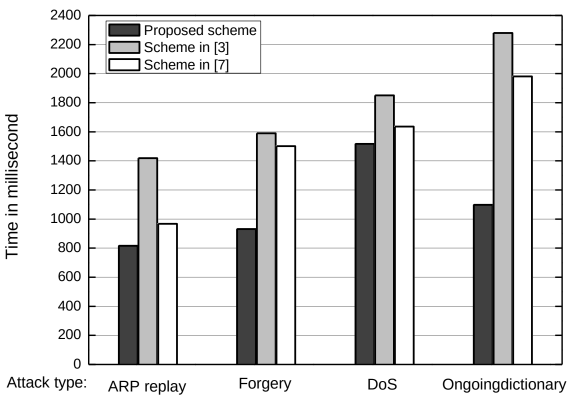


Fig. 8. Time consumption.

Storing the proposed scheme will of course require memory consumption. As shown in Fig. 9, as a rule, the memory consumption required by our scheme is lower than when the rules of UCON and attack detection are separate, which shows that our scheme has advantages in memory consumption.

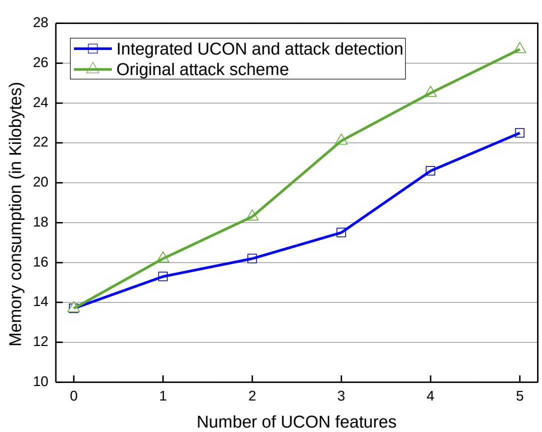


Fig. 9. Memory consumption.

B. *Attack Detection Capability*

We use these metrics to evaluate the system: the detection rate δ evaluates the overall attack detection performance, which is formally defined by

$$\delta = x/n \tag{15}$$

where x is the number of attacks that are detected, and n is the total number of attacks that actually occur.

By using the discrete event system specification (DEVS) Formalism [35], an attack detection simulation was performed to serve as a platform for evaluation. 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 in [6] and [11] are shown in Fig. 10. In that figure, the detection rate of the proposed scheme is obviously higher than that of the more typical compared schemes, especially for unknown ongoing dictionary attacks. This is because the cooperation between the low level attack detection and high level attack detection.

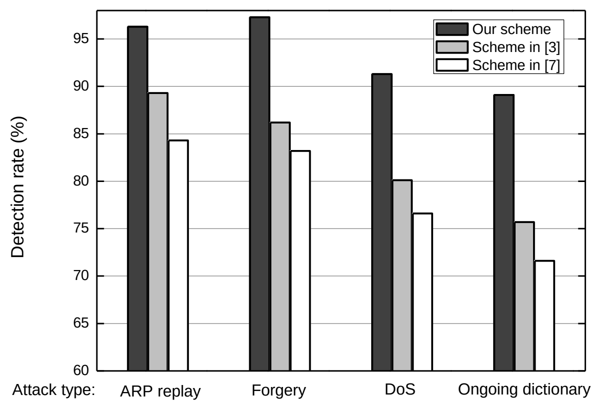


Fig. 10. Attack detection rate.

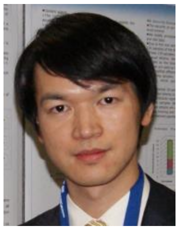
VIII. Conclusions

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

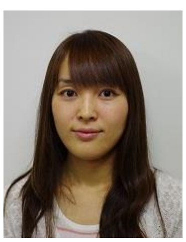
[1] K. Ota, M. Dong, J. Wang, S. Guo, Z. Cheng and M. Guo, "Dynamic Itinerary Planning for Mobile Agents with a Content-Specific Approach in Wireless Sensor Networks," in

Proc. of IEEE 72nd Vehicular Technology Conference Fall (VTC 2010-Fall), Ottawa, Canada, 2010.
[2] 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.
[3] L. Guo, J. Wu, Z. Xia and J. Li, "Proposed Security Mechanism for XMPP-based Communications of ISO/IEC/IEEE 21451 Sensor Networks," IEEE Sensors Journal, vol. 15, no. 5, pp. 2577-2586, Mar. 2015.
[4] M. Dong, K. Ota, L. T. Yang, S. Chang, H. Zhu, Z. Zhou, "Mobile Agent-based Energy-Aware and User-Centric Data Collection in Wireless Sensor Networks," Computer Networks, vol. 74, pp. 58-70, Spet. 2014.
[5] Y. Zhang, Y. Ren, "Distributed Privacy-Preserving Access Control in Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1427-1438, 2012.
[6] 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.
[7] 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.
[8] E. Y. Vasserman, N. Hopper, “Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks,” IEEE Transactions on Mobile Computing, vol. 12, no. 2, pp. 318-332, 2013.
[9] 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.
[10] P. Yi, T. Zhu, Q. Zhang, Y. Wu, J. Li, "Green Firewall: An Energy-Efficient Intrusion Prevention Mechanism in Wireless Sensor Network," in Proc. of IEEE Global Communications Conference (GLOBECOM 2012), Anaheim, California, USA ,2012.
[11] 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.
[12] J. Harbin, P. Mitchell, D. Pearce, "Wireless Sensor Network Wormhole Avoidance Using Disturbance-Based Routing Schemes," in the proc. IEEE International Symposium on Wireless Communication Systems(ISWCS 2009), Italy, 2009.
[13] C. Lin, J. Leneutre, "A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks," IEEE Transactions ON Information Forensics and Security, vol. 4, no. 2, pp. 165-178, 2009.
[14] W. Lu, M. Tavallaee, A. A. Ghorbani, "Detecting Network Anomalies Using Different Wavelet Basis Functions," In Proc. of The 6th Communication Networks and Services Research Conference, Halifax, Nova Scotia, Canada, 2008.
[15] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, S. Dubus, A. Martin, "Success Likelihood of Ongoing Attacks for Intrusion Detection and Response Systems," In Proc. of International Conference on Computational Science and Engineering (CSE 2009), Vancouver, Canada, 2009.
[16] C. Chen, J. Ma, K. Yu, "Designing Energy-Efficient Wireless Sensor Networks with Mobile Sinks," in the Proc. of Workshop on World-Sensor-Web at the 4th ACM Conference on Embedded Networked Sensor Systems (SenSys 2006), Boulder, Colorado, USA, 2006.
[17] J. Zhang, V. Varadharajan, "A New Security Scheme for Wireless Sensor Networks," in the proc. IEEE Global Communications Conference (GLOBECOM 2008), New Orleans, LA, USA, 2008.
[18] B. Thuraisingham, "Secure Sensor Information Management and Mining," IEEE Signal Processing Magazine, vol. 21, no. 3, pp. 14–19, 2004.
[19] Y. Ohsawa, P. McBurney eds.,: Chance discovery (Advanced information processing). Springer-Verlag, 2003.
[20] Ohsawa Y., N. E. Benson, M. Yachida, "KeyGraph: Automatic ln Indexing by Cooccurrence Graph Based on Building Construction Metaphor," in Proc. IEEE International Forum on Research and Technology Advances in Digital Libraries Conference，(ADL 98)，Santa Barbara, CA , 1998.
[21] X. Zhang, F. P. Presicce, R. Sandhu, "Formal Model and Policy Specification of Usage Control," ACM Transactions on Information and System Security, vol. 8, no. 4, pp. 351–387, 2005.
[22] Z. Su and Q. Xu, "Content Distribution over Content Centric Mobile Social Networks in 5G," IEEE Communications Magazine, vol. 53, no. 6, pp. 66-72, 2015.
[23] Z. Su, Q. Xu, H. Zhu, Y. Wang, "A Novel Design for Content Delivery over Software Defined Mobile Social Networks," IEEE Network, vol. 29, no. 4, 62-67, 2015.
[24] Q. Xu, Z. Su, and S. Guo, "A Game Theoretical Incentive Scheme for Relay Selection Services in Mobile Social Networks," IEEE Transactions on Vehicular Technology, vol. PP, no. 99, 2015.
[25] 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.
[26] Security frameworks for open systems: Access control framework, ISO/IEC Standard 10181-3 (1996).
[27] Y. Ohsawa, “Data Crystallization: A aroject beyond Chance Discovery for Discovering Unobservable Events, “ in Proc. of IEEE International Conference on Granular Computing (GrC 2005), Beijing, China, 2005.
[28] G. Anastasi, E. Borgia, M. Conti, E. Gregori, A. Passarella, "Understanding the Real Behavior of Mote and 802.11 Ad Hoc Networks: an Experimental Approach," Pervasive and Mobile Computing (Elsevier), vol. 1, no. 2, pp.237-256, 2005.
[29] J. Park and R. Sandhu, “The ABC Core Model for Usage Control: Integrating Authorizations, oBligations, and Conditions,” ACM Transactions on Information and System Security, vol. 2, no. 3, pp. 1-46, 2002.
[30] IEEE 802.11-1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer Extension in the 2.4 GHz Band , 1999.
[31] W. Lee, S. J. Stolfo, "A Framework for Constructing Features and Models for Intrusion Detection Systems," ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 227–261, 2000.
[32] J. R. Quinlan, "Induction of Decision Trees," Machine Learning, vol. 1, pp. 81-106 (1986).
[33] A. Bittau, M. Handley, J. Lackey, "The Final Nail in WEP’s Coffin," Proc. of IEEE Symposium Security and Privacy, 2006.
[34] Backtrack 4, http://www.backtrack-linux.org/
[35] 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, 2000.



Jun Wu is an Associate Professor of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China. He obtained his PH.D. Degree in Information and Telecommunication Studies at Waseda University, Japan. He was a postdoctoral researcher for the Research Institute for Secure Systems (RISEC), National Institute of Advanced Industrial Science and Technology (AIST), Japan, from 2011 to 2012. He worked as a researcher for the Global Information and Telecommunication Institute (GITI), Waseda University, Japan, from 2011 to 2013. His research interests include the advanced computation and communications techniques of smart sensors, wireless communication systems, industrial control systems, wireless sensor networks, smart grids, and more. He has hosted and participated in several research projects for the National Natural Science Foundation of China, National 863 Plan and 973 Plan projects, etc. He has been a Guest Editor for the IEEE Sensors Journal and a TPC Member of several international conferences including WINCON 2011, GLOBECOM 2015, etc. He is a member of IEEE.

Mianxiong Dong (M'13) received B.S., M.S. and Ph.D. in Computer Science and Engineering from The University of Aizu, Japan. He is currently an Assistant Professor with Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan. He wasa Researcherwith National Institute of Information and Communications Technology (NICT),Japan. He was a JSPS Research Fellow with School of Computer Scienceand Engineering, The University of Aizu, Japan and was a visitingscholar with BBCR group at University of Waterloo, Canada supported byJSPS Excellent Young Researcher Overseas Visit Program from April 2010to August 2011. From January 2007 to March 2007, he was a visitingscholar of West Virginia University, USA. Dr. Dong was selected as Foreigner ResearchFellow (A total of 3 recipients all over Japan) by NEC C&C Foundation in 2011. He is the Best Paper Award winner of IEEE HPCC2008 and IEEE ICESS 2008. Dr. Dong is currently a research scientist with A3Foresight Program (2011-2014) funded by Japan Society for thePromotion of Sciences (JSPS), NSFC of China, and NRF of Korea. Hisresearch interests include wireless sensor networks, vehicular ad-hocnetworks and wireless security.



Kaoru Ota (M'12) received M.S. degree in Computer Science from Oklahoma StateUniversity, USA in 2008 and Ph.D. degree in Computer Science andEngineering from The University of Aizu, Japan in 2012. She iscurrently an Assistant Professor with Department of Information andElectronic Engineering, Muroran Institute of Technology, Japan. FromMarch 2010 to March 2011, she was a visiting scholar with BBCR groupat University of Waterloo, Canada. Also she was a prestigious JapanSociety of the Promotion of Science (JSPS) research fellow withGraduate School of Information Sciences at Tohoku University, Japanfrom April 2012 to April 2013. Dr. Ota is a recipient of JSPS Grant-in-Aid for Research ActivityStart-up in 2013. She has joined JSPS A3 foresight program as one ofprimary researchers since 2011 which is supported by Japanese, Chineseand Korean government. She serves as a Guest Editor of IEICE Transactions onInformation and Systems, Special Section on Frontiers of Internet ofThings 2014, Editor of Peer-to-Peer Networking and Applications (Springer), Journal of Cyber-Physical Systems, and International Journal of Embedded Systems. Dr. Ota has actively involved ininternational conferences in present and past. Currently she is thePublicity Co-chair of the 2014 ICC workshop on Secure Networking andForensic Computing and 2014 IEEE ICCC Workshop on Internet of Things.Her research interests include wireless sensor networks, vehicular networks, and ubiquitous computing.

Chunxiao Li holds a B.E. degree in electronics and information science and technology from Shaanxi Normal University, Xi'an, China, (2006) and an M.E. degree in communications engineering from the East China Normal University, Shanghai, China (2009). She received her Ph.D. degree from Waseda University, Japan in 2012 and is now an associate professor at the College of Information Engineering of Yangzhou University, China, where she has worked since September, 2012. Her research interests are related to Intelligent Transportation System, dynamic traffic light control, eco-driving, VANET and Vehicle to Grid.