On Data Gathering and Security in Wireless Sensor Networks

Hidehisa Nakayama*, Nirwan Ansari†, Abbas Jamalipour‡, Yoshiaki Nemoto*, and Nei Kato*
*Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan
†Advanced Networking Laboratory, ECE Department, NJIT, Newark, NJ 07012, USA
‡School of Electrical and Information Engineering, University of Sydney, Sydney, NSW 2006, Australia

***Abstract*— Expected growth in use and implementation of wireless sensor networks (WSNs) in different environments and for different applications creates new security challenges. In WSNs, a malicious node may initiate incorrect path information, change the contents of data packets, and even hijack one or more genuine network nodes. As the network reliability completely depends on individual nodes' presence and collaborations with others, those malicious behaviors could halt WSNs. In this paper, the WSNs will be first categorized into three types in accordance to the way that data are collected. After a succinct summarization of each data gathering scheme, a comprehensive survey on security problems will be presented. Finally, some general design guidelines against typical attacks along with our proposals in WSNs will be provided. Unsolved problems and further studies will also be discussed.**

I. INTRODUCTION

With the needs for sensor networks on the rise, the security issues have become one of the major concerns in their practical deployments. Sensor networks may encounter various security threats at different protocol layers once they are scattered in hazardous environments. In an adversarial environment, sensors can be even captured and subsequently totally replaced with hostile nodes which can be manipulated by adversaries to eavesdrop or interrupt traffic flows.

Sensor networks can be classified into three types in accordance to the way that data are collected. The first type is that each sensor is equipped with equal ability such as computational power and storage capacity so that homogenous networks are formed. Data gathering in this type is based on the structure of data dissemination. Flat and hierarchical are two representative structures being widely studied for data dissemination and gathering in homogenous networks [1], [2]. While these mechanisms are concise as to form the rudimentary routing protocols in homogenous Wireless Sensor Networks (WSNs), the ability required for conveying data is considered inadequate, owing to the limited resources on each sensor.

With advances in signal processing and Micro-Electro-Mechanical Systems (MEMS) technologies, sophisticated sensors with low cost and more computing power are emerging. As a result of this advancement, data gathering can be executed in a different manner, in which the mobile nodes which also known as mobile sinks, are introduced [3]. In the sense that the sinks and sensors are playing different roles with their different embedded processing and communicating capabilities, this kind of sensor networks can be treated as heterogeneous. We regard these heterogeneous sensor networks as the second type. In these networks, high performance sensor nodes assume the role of sinks in collecting data from normal sensors.

Aiming at further improving the efficiency of sensor networks, according to circumstances, some high performance sensor nodes can be even mounted on robots or unmanned airplanes. In this regard, data gathering with mobile sinks has been proposed [3]. In this scheme, mobile sinks move randomly in the area of deployment of a sensor network, pick up data directly from sensors, or use some surrounding sensor nodes to relay the data to them.

The idea of using several mobile sinks can further improve the performance when these agents work in a cooperative way. This leads to the fastest data gathering scheme referred to as mobile relay by which the data can be collected in a real time manner. Data transferred in this case will be relayed by several mobile sinks.

From the point of view that the performance of a sink is comparable with those of nodes used in ad hoc networks [4], the conventional and well studied routing algorithms for ad hoc networks, say AODV and OLSR, were adopted as the routing protocols. In this paper, we treat this hybrid scheme combining ad hoc techniques as the third type of sensor networks. The third type can achieve longer lifetime and can also improve the efficiency of data gathering.

Latent threats to sensor networks are diverse. Network attacks may occur from the physical layer to the transportation layer depending on what the attacks are attempting to attain. In the physical layer, jamming attacks are considered as the most serious attacks [5]. Jamming attacks generally use the same radio frequency to interfere with other sensors. This can be executed even without knowing the coding scheme that the sensor network has adopted.

In the link layer, collision is a well-known attack affecting sensor networks seriously. A malicious node may intentionally transmit data colliding with other normal nodes. This way, the nodes surrounding the attacker cannot assemble the packets. Another tricky attack in the link layer is the misuse of the MAC protocol to occupy the transmission slots as to prevent the normal nodes from sending their data timely. This situation can occur when a node is compromised with injected malicious codes. In this case, the compromised node can behave as if it was a normal node.

Most annoying attacks are those targeted at the network layer. In a sensor network where all nodes cannot be controlled remotely once scattered, a malicious node can deliberately broadcast forged routing information to deprive the normal nodes of their connections. Typical attacks in the network layer are Sinkhole [6], Sybil [5], [7], and Wormhole [6] attacks. These attacks will result in information leak or route interruption. To establish the reliable connections between sensors, secure routing based on key management protocols has been proposed [6]. While a secure routing scheme can prevent routing attacks from the outside, it is still helpless against inside attacks or from compromised nodes. The complexity of secure routing remains a challenging issue. In this paper, we mainly focus on the most serious cases in which the attacks are from the inside or compromised nodes. In other words, we assume the case that the attackers possess the secret key of a legitimate node, and hence can communicate with its surrounding nodes.

In the transport layer, the most notorious attack is the flooding attack. A compromised node with more computational power and energy can flood any node with a large volume of data or persistently request a specific node to send the stored data. This will occupy the processing ability of the target node and exhaust its power quickly.

The extent of damage caused by attacks is contingent upon the means of the data gathering and dissemination. For example, in a flat network structure, a single attacker may not be powerful enough to execute an attack to paralyze the whole network. On the contrary, in hierarchically structured networks, an attack against the root node would be sufficient to cause a serious damage to the whole network. In a heterogeneous network, one can easily imagine that an attacker, by exerting as much damage as it can on sinks, can sabotage the whole networks. In a hybrid network with ad hoc nodes, attacking the ad-hoc nodes is the most effective way to influence the whole network.

Needless to say, different network structures need different defensive measures. Generally speaking, to securing reliable data in homogenous networks, detecting attacks and circumventing the risky areas or paths are the most important. For heterogeneous networks, preventing sinks from attacks can relieve the whole network from suffering severe damage. To secure hybrid networks, attack detection methods for ad hoc networks might be effectively applied/adopted. Statistical approaches such as dynamic learning which can differentiate abnormality from normal states are viable options [8].

The rest of this paper is organized as follows. In Section 2, three major data gathering schemes are introduced. In Section 3, we will focus on the typical attacks threatening these schemes. In Section 4, some basic ideas for detecting attacks and methods in reducing the impact of attacks on networks are discussed. In Section 5, conclusions and some future works will be presented.

II. MAJOR DATA GATHERING SCHMES IN WSNs

Fig. 1 shows the general structure of a WSN. In Fig. 1, we assume that an administrator distributes sensors to monitor the targeted area, and sensors do not move afterwards. Sinks play the role as data gathering nodes, and can move if necessary. An administrator can access WSN and obtain sensing information through the gateway node, which is also called a base station (BS).

In Fig. 1 (a), in homogenous WSN, sensors and sinks are furnished with almost the same resources. In Fig. 1 (b), sensors are equipped with uniform resources, but sinks are furnished with more resources for heterogeneous WSN. There are two triggers in data gathering: query based and event driven. Fig. 1 expresses the query based type where white and black arrows indicate query and data flows, respectively. In case of an event driven, there will be no queries.

A. Data gathering in homogenous WSNs

The simplest model is one with a sink being the base station. In this model, the data propagate from sensors to the sink directly or via multi-hop communications. For the flat-type routing, the most typical protocols are SPIN and Directed Diffusion, whereas for the hierarchical routing, LEACH and PEGASIS are common [9].

B. Data gathering in heterogeneous WSNs

Sometimes, sensors may be distributed sparsely, and the distance between any two sensors can be long. The long distance among sensors implies that more energy will be consumed during communication. Meanwhile, sensors need to perform long-term sensing and communication as long as possible. As a result, the communication between sensors and sinks using not only single-hop but also multi-hop poses a great challenge. In response to such requirements, there have been many proposals concerning the ”mobile sink” model, in which sinks move around in the sensing area and aggregate data from sensors. These models are composed of a few resource-rich mobile sinks and a large number of static/semi-static sensors. As shown in many experimental results (for

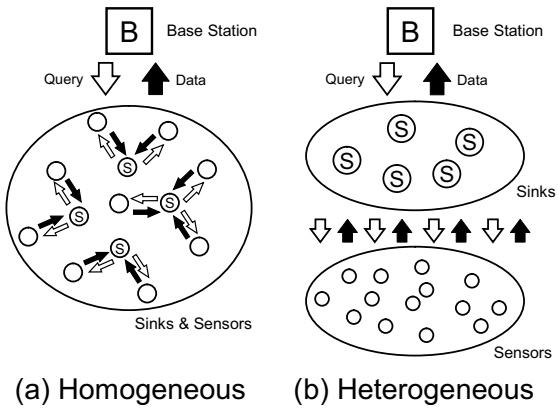

Fig. 1. WSN architecture

example [10]), data gathering with mobile sinks is able to prolong the lifetime of the system. In this paper, we discuss three functional categories.

- **Mobile Relay:** Use multi-hop communication between sensors and sinks. Sinks can move around in the sensing area.
- **Mobile Sink with Single-hop:** Use single-hop communication between sensors and sinks. Sinks can move around in the sensing area.
- **Mobile Sink with Multi-hop:** Use multi-hop communication between sensors and sinks. Sinks can move around in the sensing area.

Mobile Relay:

Mobile Relay is similar to the Home Agent in Mobile IP. WSN sets relay nodes which can cover the entire sensing area. The relay nodes update the location of mobile sinks so that the relay node can transfer data by multi-hop propagation from sensors to the corresponding sink.

Mobile Sink with Single-hop:

Mobile sensors have been researched in Habitat Monitoring. By borrowing the mobility of animals, a mobile sensor, which is parasitic on animals, moves around in the targeted area and obtains the information without spending the energy. By the same token, mobile sinks with rich resources can also move around in the entire area and communicate with sensors.

Mobile Sink with Multi-hop:

Trajectory control is an effective operation for a mobile sink to gather data from sensors, but this will lead to the sink deployment problem. By exploiting sink mobility, sensors can communicate via a sensor-specific protocol. Meanwhile multi-hop communication increases complexity as compared to single-hop. Therefore, it is necessary to consider the trade-off of communication loads between sensors and sinks.

C. Data Gathering in MANET

Mobile Adhoc Networks (MANETs) assume that every node is able to move at their own pace. So even though WSN has low connectivity, the route from a source to a destination can still be established by using MANET protocols. Accordingly, if the location of sensors is unpredictable or in case the sensors cannot communicate with each other on their own, it is reasonable to tailor techniques proposed for MANETs for WSNs. However, in reality, most sensors are predictable because sensors are intentionally distributed. As pointed out in [11], a mobile sink prefers a hybrid architecture, by which a mobile sink can communicate with other sensors using a WSN protocol and with other sinks using a MANET protocol as shown in Fig. 2.

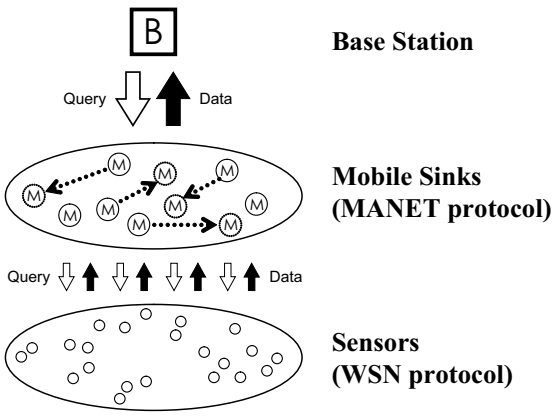

Fig. 2. MANETs for Supporting WSNs

III. TYPICAL ATTACKS AGAINST DIFFERENT DATA GATHERING SCHEMES

In this section, several typical attacks ranging from the physical layer to the transport layer will be introduced. Concretely, jamming and collision attacks in the physical and link layer, sinkhole, sybil, and wormhole attacks in the routing layer, and flooding attacks in the transport layer, as shown in Fig. 3, will be described. Note that launching these attacks sometimes also entails great expenses on the adversaries. Assesing severity of attacks depends on the assortment of applications and how accessible and powerful the adversaries are.

A. Physical and Link Layer

Jamming and collision attacks are two representative attacks in the physical and link layer. Launching these attacks near the BS or close to the roots in a tree-like data gathering architecture can cause serious damages to the whole WSNs.

Jamming is a typical attack instigated in the physical layer. An attacker can transmit a jamming signal near the targeted node, or scatter the malicious nodes randomly in the targeted sensor network field. In wireless networks, jamming technologies to intentionally blocking various radio signals have been widely deployed for military applications. It is easy to imagine that these technologies might be misused.

To alleviate the damage of these physical layer attacks, frequency-hopping spread spectrum (FHSS) and code spreading are common countermeasures [12]. However, these approaches are not readily applicable in WSNs not only due to

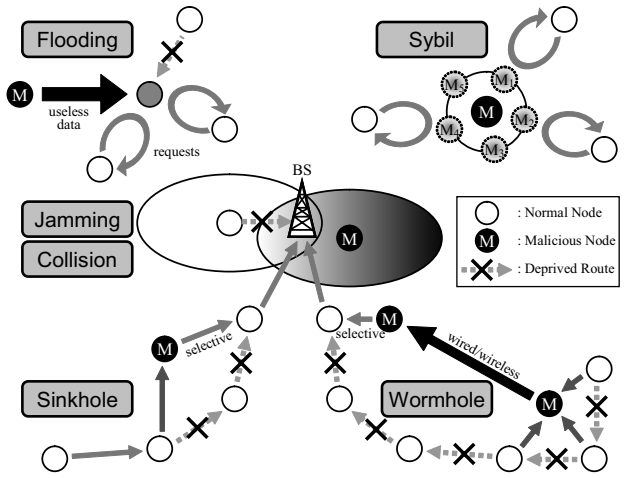

Fig. 3. Various Types of Attack

the cost and power problems but also the uncertainty of the attack types. Besides these approaches, the active approach, which first detects the malicious nodes, and then gets rid of them from the sensor field, can be considered the most viable option, given that the sensor fields are accessible by ad-hoc nodes or mobile agents.

Collision is the typical type of attacks in the link layer. Collision can be further divided into two types. The first one is that the malicious node attempts to transmit its data at any timing to cause partial data collision. When a malicious node disobeys the media access control (MAC) protocol, and sends its packets frequently, serious problems like network congestion may be incurred. The second type of collision attacks is more devastating in which a malicious node pretends to be a normal node and seizes most of the access privileges to prevent other nodes from sending their data. The potential way of detecting this kind of attacks is to observe the node behavior statistically to see, for example, if the sending frequency of a certain node deviates largely from the others.

B. Network and Routing Layer

Unlike the physical and link layer attacks whose misconduct might be conceived by the neighboring nodes to some extent, the most repulsive attacks are instigated in the network and routing layer. By routing attacks, the attackers can maneuver the route to eavesdrop on the packets or deliberately isolate specific nodes even without being noticed by its surrounding nodes. Meanwhile, detecting these attacks is a challenging task because it is difficult to differentiate the behavior of those malicious nodes from the normal ones in most cases. The typical attacks in this layer are sinkhole, sybil, and wormholes attacks. The characteristics of these attacks and their implications will be explained below.

In a sinkhole attack, a compromised node sends various false routing information to cheat its surrounding nodes as if it were the most attractive or reliable node in terms of delay, bandwidth, and remaining battery. How to deceive the surrounding nodes into authenticating it as a trustful node depends on the data dissemination and gathering scheme of the targeted WSN. In general, the compromised node may first pretend to be a normal node and overstate its performance regarding the relay ability as an intermediate node. Once it gains the trust of its surrounding nodes (its surrounding nodes have selected it as the exclusive relay node), then it can start misusing the traffic forwarded from those neighboring nodes. The misuse includes packet dropping, intentional forwarding, and eavesdropping.

In a sybil attack, a compromised node changes deliberately its identities and keeps sending the false routing information continuously to its surrounding nodes. A sybil attack can affect many aspects of WSNs including the routing property.

In a wormhole attack, two malicious nodes with strong transmission power collaborate with each other to form a tunnel across a wide area. The worst scenario is when one of the malicious nodes is hiding somewhere near the BS, in which case the attack will harm the WSNs the most. Since the malicious node near the BS can create short delay links both with BS and its counterpart on purpose, this tunnel link will appear to be very attractive to their surrounding nodes. As a result, traffic from most of the vicinal nodes will be drawn into this tunnel. Wormhole can also be misused in combination with other attacks such as sinkhole and sybil. It can also instigate powerful flooding attacks.

Detecting the wormhole attack is not an easy task. Provided that inbound and outbound traffic of each node in WSNs can be overheard by its neighboring nodes, statistical analysis which will be introduced later can become a promising strategy in the future.

C. Transport Layer

In the transport layer, flooding is the most annoying attack. Flooding can be categorized into two types. The first type is one in which the attackers keep sending the useless data continuously to the target node. When the target node has to receive excessive amount of data than its capacity, it will be totally congested. The second type is that the attackers keep sending requests to the target node. In this case, the target node will be forced to consume a large quantity of power replying to the requests. As a result, the target node will die off quickly.

Flooding attacks have been studied in depth so far as they have also posed a great threat to Internet and ad hoc networks. Some techniques, which will be described in Section 4.3, can be tailored from the previous research for the WSNs environment.

IV. DESIGNING COUNTERMEASURES AGAINST SERIOUS ATTACKS IN WSNs

After deployment, except a small number of mobile sinks, most sensors will be left at their initial deployed positions without being attended until their batteries run out. Since recharging or repairing a compromised sensor might be unrealistic, furnishing sensors with cryptography to maintain secure paths is first considered. This countermeasure can prevent outside attacks from joining the WSNs. However, designing a hard-to-crack cryptography on sensors with limited communication, processing, and storage capacity is almost impossible. Also, the cases, where an attack is from inside or from a compromised node, should be addressed. Minimizing the impact of attacks and guaranteeing the data integrity by avoiding gathering information from the affected areas is also essential. To this end, designing a path for mobile sinks to circumvent the damaged area is useful. Besides the above two conceivable means, another powerful mean resorting to the implementation of attack detection on mobile sinks can also be explored. In this section, we will succinctly introduce these countermeasures.

A. Reducing the risk of outside attacks by applying cryptography

Public key and symmetric key cryptography are the two main cryptographic methods intended for WSNs. Public key cryptography, also known as asymmetric key cryptography,

was proposed by Whitfield Diffie and Martin E. Hellman in 1976. RSA and ECC are some most well-known public key algorithms in which a pair of keys is used in encryption and decryption. While the public key infrastructure can be appropriately established for Internet where resources such as bandwidth, processing ability, and the authentication server are readily available, it is difficult to apply such expensive and complicated scheme to WSNs. For this reason, rather than applying the public key cryptography, the symmetric key cryptography has been considered more suitable for WSNs.

There are five representative symmetric encryption schemes as symmetric key cryptography, RC4, IDEA, SHA-1, and MD5. Unless sensors have access to the designated keys, they cannot exchange data with each other. In a WSN, key management is extremely important.

Key management protocols hinge upon the network structure. In the simplest scheme, i.e., the centralized key management scheme, there is only one entity being assigned to take charge of key distribution [13]. The problem of this centralized scheme is its weak failure resilience.

There are two main distributed key management approaches, deterministic and probabilistic. In Reference [12], types of keys including master, pairwise, path, and cluster are listed for each method. Also, the merits and demerits in terms of scalability, resiliency, processing load, communication load, and storage load have been discussed. Distributed key management schemes are envisaged as the presently-accepted alternatives.

As mentioned before, most troublesome attacks are instigated in the network routing layer. To ensure the reliable paths in WSNs, secure routing protocols have been designed based on various key management schemes. The main purpose of secure routing is to prevent outside adversary from joining the path and gaining the control of flows. Secure routing protocols depend on the network structure which can currently be categorized into two types, flat and hierarchy. In many cases, these schemes need predistribute keys to certain members beforehand to form a reliable group for key management. In some schemes, time synchronization among sensors is also required. On the cost of power consumption, storage, and processing time, secure routing protocols can keep the route safe at some level. However, when the attacks are from the inside or from a compromised node, the secure routing protocols may become helpless.

B. Secure Data Gathering by KAT Mobility

Sensors are vulnerable to physical attacks because the monitoring area is open to everyone. When sensors are malicious or annihilated, such suspicious nodes must be dodged for data consistency gathering. Several secure schemes (e.g., SPINS [14], SIA [15], SRDA [16], and CDA [17]) have been proposed [2], [6]. In particular, to combine energy efficiency with secure data collection, Cam *et.al.* [18] have developed ESPDA (Energy-efficient and Secure Pattern-based Data-Aggregation) protocol, where the pattern code (PC) ensures the data to be collected. Each sensor node constructs a PC from environmental parameters, and the cluster-head node analyzes the PC and decides whether it receives the data from the sensor.

KAT Mobility:

In contrast to the above methods, we propose a fault-resilient scheme for data gathering with mobile sinks in heterogeneous WSNs. As pointed out in [19], if a representative node is given many roles, it will become a very attractive target for many attacks. Therefore, routine trajectories of sinks, which are following the same path with a fixed speed, should be avoided. We should determine the trajectories of sinks by the following two modules: the k-means clustering algorithm and the approximate solution for TSP (Traveling Salesman Problem) [20], [21]. Sensors are first clustered by using the k-means clustering algorithm, from which the cluster centers are designated as anchor points. Second, the migration route of sinks is determined as an approximate solution of TSP. Accordingly our new mobility is referred to as the KAT Mobility (the K-means And TSP based mobility); Fig. 4 shows an overview of these modules. Fig. 5 is an exemplary trajectory determined by KAT mobility. When sensors are compromised or sabotaged for various reasons, the route selected by using our proposed KAT mobility avoids the dangerous area, which is shown as a shaded rectangle in Fig. 5.

In addition, a mobile sink travels at a velocity that varies randomly with pauses, like a random waypoint mobility. We use the One-Phase Pull Diffusion protocol as a multihop-communication between sensors and a mobile sink. In fact, secure protocol, including CDA and ESPDA, can be employed here.

We have used the Qualnet network simulator (Ver. 3.9.5 and its extension [22], [23]) to consider the following metric $E(KB/mWhr)$, which indicates the amount of data collected from one sensor per unit energy:

$$E = \frac{\text{(Received Bytes by all sinks)}}{\text{(Consumed Energy by all sensors)} \times N} \tag{1}$$

where N is the total number of sensors.

Fig. 6 shows the performance comparisons among the three mobility models (deterministic, random waypoint, and KAT), when the number of clusters is 10. This simulation demonstrates the robustness of KAT mobility against faulty or compromised sensors.

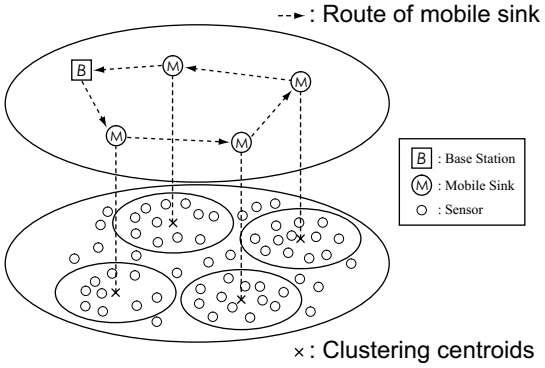

Fig. 4. Overview of proposed modules

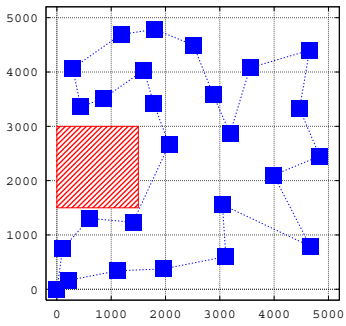

Fig. 5. Example route of KAT mobility

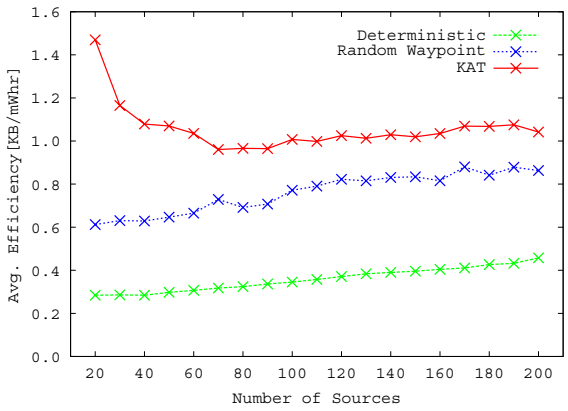

Fig. 6. Performance comparisons among the three mobility models when sensors in the given area are dead or sabotaged

C. Anomaly Detection by Projection Distance

In a monitoring field, sensors are scattered and will not move afterwards. Therefore, it is difficult to distinguish whether any attacks occurred or not. Many attempts have been proposed to prevent sensors from such attacks [6]. It is difficult to mitigate DoS (Denial of Service) in WSNs [24], because the administrator of sensors is generally isolated at a remote place. Mobile sinks equipped with anomaly detection functions are a likely viable option to tackle this problem. To detect abnormal states automatically, a statistical approach is preferable over protocol-specific countermeasures. As mentioned in Section II-B, the further development of mobile sinks may adopt MANET protocols. Similarly, in this section, given the rich resources of a mobile sink, we assume that mobile sinks can transmit statistical information other than monitored data to the base station. Accordingly, we propose anomaly detection in WSNs by projection distance, similar to our proposed countermeasures for MANETs [8].

Projection-distance:

Each node observes the amount of its own packets in a short duration, by using a time slot to count up the traffic according to its kinds. In a time slot t at node i, the network state is expressed by a p-dimensional vector, $\boldsymbol{x}_i(t)$. Consider a training data set $\boldsymbol{D}_i$ collected by node i consisting of D_i time slots ($D_i = |\boldsymbol{D}_i|$), that is, the current time interval at node

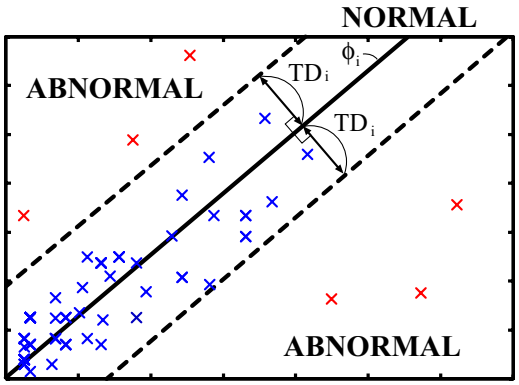

Fig. 7. Dividing projection distance into two states

i consists of D_i time slots. From Eqs. (2) and (3), we first calculate the average $\bar{\boldsymbol{x}}_i$ and covariance matrix $\boldsymbol{\Sigma}_i$ as follows:

$$\bar{\boldsymbol{x}}_i = \frac{1}{D_i}\sum_{t=1}^{D_i}\boldsymbol{x}_i(t)\,, \tag{2}$$

$$\boldsymbol{\Sigma}_i = \frac{1}{D_i}\sum_{t=1}^{D_i}(\boldsymbol{x}_i(t)-\bar{\boldsymbol{x}}_i)(\boldsymbol{x}_i(t)-\bar{\boldsymbol{x}}_i)^T\,. \tag{3}$$

From $\bar{\boldsymbol{x}}_i$ and $\boldsymbol{\Sigma}_i$, we use the Principal Component Analysis (PCA) to analyze the statistical nature of the current time interval. Using PCA, the first principal element $\boldsymbol{\phi}_i$, which reflects the approximate distribution of the learning data sets, is calculated. Here, we consider the projection distance (PD) of the current state $\boldsymbol{x}_i$ in a time slot t at node i as:

$$d(\boldsymbol{x}_i(t)) = \| \boldsymbol{x}_i(t)-\bar{\boldsymbol{x}}_i \|^2 - \boldsymbol{\phi}_i^T(\boldsymbol{x}_i(t)-\bar{\boldsymbol{x}}_i)\,. \tag{4}$$

When the PD is larger than the threshold TD_i, that is $d(\boldsymbol{x}_i(t)) > \mathrm{TD}_i$, then $d(\boldsymbol{x}_i(t))$ is considered out of the range of normal traffic, and is thus considered as abnormal. Here, the PD with the maximum value is extracted as T_i from the training data set:

$$\mathrm{TD}_i = d(\boldsymbol{x}_i(T_i)), \quad T_i = \arg\max_{t\ \boldsymbol{x}_i(t)\in\boldsymbol{D}_i} d(\boldsymbol{x}_i(t))\,. \tag{5}$$

Fig. 7 illustrates a rough image of discriminating the abnormal state from the normal state by PD in the two-dimensional ($p = 2$) case.

We shall next describe the simulation results of a set of 50 mobile sinks with a random waypoint mobility. The simulation is conducted on ns-2 [25], where mobile sinks, which are driven by the AODV routing protocol, are suffering from a malicious flooding. In case of malicious flooding, a malicious node forges the source and destination ID in the RREQ message of AODV and sends a lot of them to the WSN. This will lead to unnecessary delay and frequent packet-dropping in the WSN.

Fig. 8 illustrates the variation of PD versus time, where the simulation time is $10,000(sec)$, the break-in period is $300(sec)$ at first, and attack period is from $2,500$ to $5,000(sec)$. As we can see the attack period in Fig. 8, PD

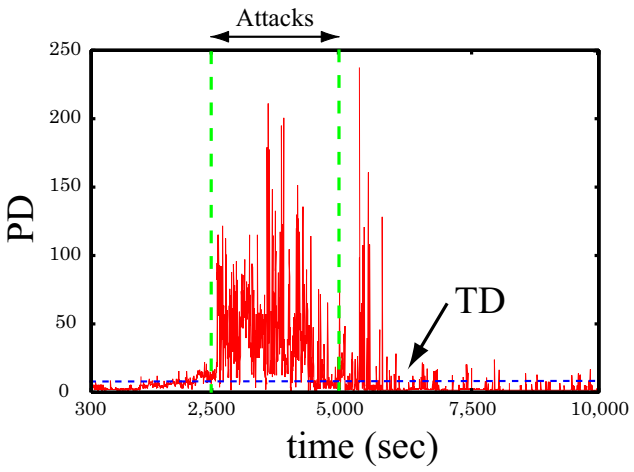

Fig. 8. Anormaly detection against Malicious flooding

is larger than the other periods. This means that a mobile sink detects the abnormal state when PD is above the threshold of the normal state (TD). However, further research is needed because there are still some false positives from $5,000$ to about $6,000(sec)$.

V. CONCLUSIONS

Unlimited potential of WSNs has been attracting a great deal of attention. To ensure a sustainable progress, a high level of security has to be accommodated. In this paper, we have surveyed the major security problems exhibited at the different layers of WSNs and discussed three types of countermeasures against various attacks. The first is using secure routing to prevent attacks mainly from the outside. The second is to mitigate the impact of attacks by efficiently circumventing the damaged area, in which we have proposed the KAT mobility model for this purpose. The third incorporates the technique used in ad hoc networks, in which we have applied PCA for anormaly detection. Designing countermeasures highly depends on the nature of WSNs including objective, scale, and level of interest by the adversaries. The most important factor in designing the countermeasures for WSNs is the cost efficiency. Given the fact that the applications of sensor networks are versatile, it is desired to address the security in great details and considerations in order to conceive an effective integrated solution. Although the perfect solution might not exist, powerful countermeasures would still be a good deterrent. With advances in sensor technologies, more security measures can be embedded in sensors and mobile sinks in the future. Many useful techniques developed in the fixed/wireless networks or ad hoc networks can be adopted.

REFERENCES

[1] I. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, Apr. 2002.

[2] R. Rajagopalan and P. Varshney, "Data-aggregation techniques in sensor networks: A survey," *IEEE Communications and Surveys and Tutorials*, vol. 8, no. 4, pp. 48–63, 2006.

[3] R. Shah, S. Roy, S. Jain, and W. Brunette, "Data mules: modeling and analysis of a three-tier architecture for sparse sensor networks." *Ad Hoc Networks*, vol. 1, no. 2–3, pp. 215–233, Sept. 2003.

[4] E. Royer and C. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Personal Communications*, vol. 6, no. 2, pp. 46–55, Apr. 1999.

[5] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 38–43, Dec. 2004.

[6] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2–3, pp. 293–315, Sept. 2003.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proc. of the 3rd International Symposium on Information Processing in Sensor Networks (IPSN 2004)*, Apr. 2004, pp. 259–268.

[8] S. Kurosawa, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "A self-adaptive intrusion detection method for aodv-based mobile ad hoc networks," in *Proc. of the 2nd IEEE Int'l. Conf. on Mobile Ad-hoc and Sensor Systems (MASS 2005)*, Nov. 2005, pp. 8B–4.

[9] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: A survey," *IEEE Trans. on Wireless Communications*, vol. 11, no. 6, pp. 6–28, Dec. 2004.

[10] I. Chatzigiannakis, A. Kinalis, and S. Nikoletseas, "Sink mobility protocols for data collection in wireless sensor networks," in *Proc. of the 4th ACM Workshop on Mobility Management and Wireless Access (MobiWac 2006)*, Oct. 2006, pp. 52–59.

[11] I. Stojmenovic, *Handbook of Sensor Networks Algorithms and Architectures*. John Wiley & Sons, 2005.

[12] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications and Surveys and Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[13] R. Pietro, L. Mancini, Y. Law, S. Etalle, and P. Havinga, "LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks," *Proc. of IEEE Int'l. Conf. on Parallel Processing Workshops (ICPPW '03)*, pp. 397–406, 2003.

[14] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "SPINS: Security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, Sept. 2002.

[15] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in *Proc. of the 1st Int'l. Conf. on Embedded Networked Sensor Systems (SenSys '03)*, Nov. 2003, pp. 255–265.

[16] H. Sanli, S. Ozdemir, and H. Cam, "SRDA: Secure reference-based data aggregation protocol for wireless sensor networks," in *Proc. of IEEE VTC Fall 2004 Conf.*, vol. 7, Sept. 2004, pp. 4650–4654.

[17] D. Westhoff, J. Girao, and M. Acharya, "Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution, and routing adaptation," *IEEE Trans. on Mobile Computing*, vol. 5, no. 10, pp. 1417–1431, Oct. 2006.

[18] H. Cam, S. Ozdemir, P. Nair, and D. Muthuavinashiappan, "ESPDA: Energy-efficient and secure pattern-based data aggregation for wireless sensor networks," in *Proc. of IEEE Sensors*, vol. 2, Oct. 2003, pp. 732–736.

[19] W. Zhang, H. Song, S. Zhu, and G. Cao, "Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks," in *Proc. of the 6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc '05)*, May 2005, pp. 378–389.

[20] D. Johnson and L. McGeoch, *The Traveling Salesman Problem: A Case Study in Local Optimization*. John Wiley & Sons, 1997.

[21] N. Ansari and E. Hou, *Computational Intelligence for Optimization*. Springer, 1997.

[22] QualNet – Scalable Network Technologies Website, `http://www.scalable-networks.com/`.

[23] B. Vasu, M. Varshney, R. Rengaswamy, M. Marina, A. Dixit, P. Aghera, M. Srivastava, and R. Bagrodia, "squalnet – a scalable simulation framework for sensor networks," in *Proc. of the 3rd International conference on Embedded networked sensor systems (SenSys '05)*, 2005, pp. 322–322.

[24] A. Wood and J. Stankovic, "Denial of service in sensor networks," *IEEE Computer Magazine*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[25] The Network Simulator - ns, `http://nsnam.isi.edu/nsnam/`.