LEDS - An innovative corridor of data security in WSN

Chetana V. Samundre
Research Scholar, Electronics and communication
P.I.ET
Nagpur (M.S.), India
e-mail: samundre.chetana@gmail.com

Prof.Mr.A.D.Bijwe
Assistant Professor, Electronics and communication
P.I.E.T
Nagpur (M.S.), India
e-mail: bijweabhijit@rediffmail.com

Abstract **-** Recently, WSNs have drawn a lot of attention due to their broad applications in both military and civilian domains. Data security is essential to the success of WSN applications, exclusively for those mission-critical applications working in unattended and even hostile environments which may be exposed to several attacks. This inspired the research on Data security for WSNs. Attacks due to node compromise include Denial of service (DoS) attacks such as selective forwarding attacks and report disruption attacks. Nearby many techniques have been proposed in the literature for data security. Hop-hop security works well when assuming a uniform wireless communication pattern and this security designs provides only hop-hop security. Node to sink communication is the dominant communication pattern in WSNs and hop-hop security design is not sufficient as it is exposed to several attacks due to node compromise. Location aware end-end data security (LEDS) provides end-end security.

Keywords-*Data security, end-to-end, DoSattack, wireless sensor network*

*****

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of a large number of spatially distributed sensor nodes. These sensor nodes can be easily established at strategic regions at a low cost. Provided with various types of sensors, sensor nodes cooperate with each other to monitor physical or environmental conditions, such as temperature, vibration, sound, image, pressure, motion or pollutants. Each sensor node is also equipped with a radio transceiver or other wireless communication device, a microprocessor, and an energy source (e.g., a battery). However, providing satisfactory security protection in WSNs has ever been a challenging task due to various network & resource constraints and malicious attacks.

The sensor nodes and the base stations are the major elements of WSN. These both can be abstracted as the 'sensing cells' and the 'brain' of the network, respectively. Security compromise of sensor nodes is one of the most severe security threats in WSNs due to their lack of tamper resistance [1]. In WSNs, the attacker could compromise multiple nodes to obtain their carried keying material and control them and thus is able to intercept data transmitted through these nodes thereafter. As the number of compromised nodes grows, communication links between uncompromised nodes might also be compromised through malicious cryptanalysis. Thus, this type of attack could lead to severe data confidentiality compromise in WSNs. Furthermore, the attacker may use compromised nodes to inject bogus data traffic in WSNs.

II. WIRELESS SENSOR NETWORK

Wireless sensor networks composed of a large number of sensor nodes. Sensor nodes are typically small, low cost, low power devices. Sensor nodess perform the functionality such as sense/monitor its local environment, perform limited data processing, and communicate on short distance. A WSN usually also contains a "sink" node(s) which collects data from sensor nodes and connects the WSN to the outside world. Wireless sensor networks (WSNs) are rapidly growing in their importance and relevance to both the research community and the public at large. A distributed wireless sensor network is formed by a large number of tiny and inexpensive sensor nodes. These nodes are typically resource constrained, with limited energy lifetime, low-power microsensors and actuators, slow embedded processors, limited memory, and low-bandwidth radios.

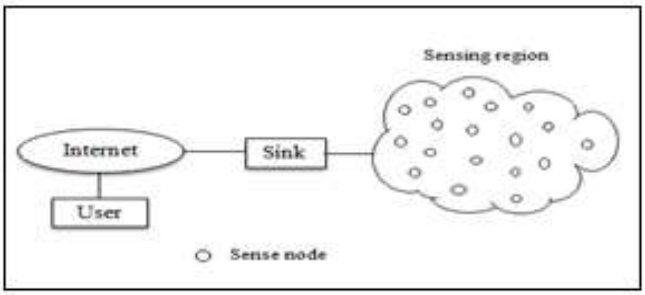

Fig. 1.Sensor network architecture.

The following unique features of WSNs make it particularly challenging to protect communication security in WSNs.

A. Resource Constraints:

Small sensors only have limited communication and computation capabilities, which makes it difficult to implement expensive security operations for WSNs. This precludes the direct transplantation of the existing security designs aimed for traditional wireless networks, where network nodes are much more powerful devices. Sensor nodes are battery-powered, having only limited energy supply. This again requires the security design to be efficient regarding both communication and computation overheads. In most cases, sensors only have very limited memory spaces, which further narrows down the security design choices. All these resource constraints require that the security design can only be efficient and lightweight; otherwise it will not be practical for WSNs.

B. Network Constraints:

WSNs use wireless open channel, therefore an adversary can easily eavesdrop all the network communications, as well as arbitrarily injecting messages and launching jamming attacks at different network layers. This means that the security design has to take into account both passive and active attacks. WSNs are distributed in nature, therefore centralized security solutions cannot be an option for WSNs. This also means that WSNs are vulnerable to various DoS attacks. WSNs are often very large in scale, which in turn imposes scalability requirement on the security design.

C. Malicious Attacks:

Give the large scale of the WSNs, it is impractical to protect or monitor each individual sensor node physically. In addition, sensors are also not tamper resistant. Therefore, the adversary may capture and compromise a certain number of sensor nodes without being noticed and obtain all the secrets stored on these sensors. The adversary is thus able to launch a variety of malicious insider attacks against the network through these compromised nodes in addition to outsider attacks. For example, the compromised nodes may report bogus observations in order to mislead the network owner or users; they may also discard important messages such as data reports in order to hide some critical events from being noticed. All these attacks could cause severe results that may disable network functionality at least temporarily. Hence, it is highly important for the security design to be robust against sensor compromise and against both outsider and insider attacks.

Despite the importance, providing satisfactory security protection in WSNs has never been an easy task. This is because sensor networks not only suffer from various malicious attacks; but also are subject to many resource and network constraints as compared to traditional wireless networks. This motivates the research data security for WSNs.

III. DATA SECURITY

One of the most severe security threats in WSNs is security compromise of sensor nodes due to their lack of tamper resistance. In WSNs, the attacker could compromise multiple nodes to obtain their carried keying materials and control them, and thus is able to intercept data transmitted through these nodes thereafter. As the number of compromised nodes grows, communication links between uncompromised nodes might also be compromised through malicious cryptanalysis. Hence, this type of attacks could lead to severe data confidentiality compromise in WSNs. Furthermore, the attacker may use compromised nodes to inject bogus data traffic in WSNs. In such attacks, compromised nodes pretend to have detected an event of interest within their vicinity, or simply fabricate a bogus event report claiming a non-existing event at an arbitrary location. Such *insider* attacks can severely damage network function and result in the failure of mission-critical applications. Such attacks also induce network congestion and wireless contention, and waste the scarce network resources such as energy and bandwidth, hence, severely affecting both data authenticity and availability. Lastly, the attacker could also use compromised nodes to launch selective forwarding attack, in which case compromised nodes selectively drop the going-through data traffic and thus data availability can be severely damaged. The existence of aforementioned attacks, together with the inherent constraints of sensor nodes, makes it rather challenging to provide satisfying data security in WSNs with respect to all its three aspects, i.e., confidentiality, authenticity and availability.

Recent research has seen a growing body of work on security designs for WSNs [2], [3], [4], [6], [7], [8], [10]. Due to the resource constraint, most of the proposals are based on symmetric cryptography and only provide data authenticity and/or confidentiality in a hop-by-hop manner. End-to-end encryption/ authentication is considered less feasible, particular in a WSN consisting of a large number of nodes. However, lack of the end-to-end security guarantee could make WSNs particularly vulnerable to the aforementioned attacks in many applications, where node-to-sink communication is the dominant communication pattern. This could give the attacker the advantage to obtain/manipulate its desired data at a much less effort

without having to compromise a large number of nodes. To make things worse, existing security designs are highly vulnerable to many types of DoS attacks, such as report disruption attacks and selective forwarding attacks.

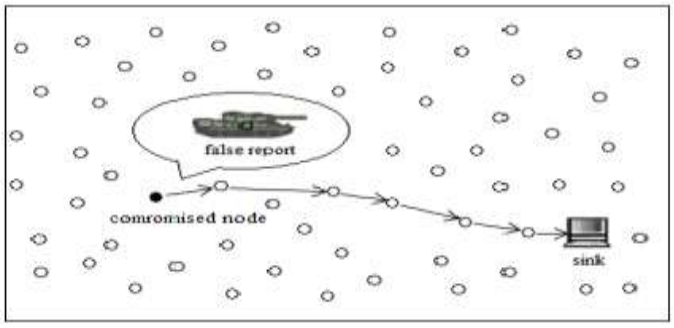

Fig. 2. Node injects false report in various locations and that false report cause false alarms. In delivering false reports energy and bandwidth could be wasted. The user may also miss a real event.

A. Data Security Requirements In Wsns

Data should be accessible only to authorized entities (usually the sink in WSNs). It should be genuine, and should be always available upon request to the authorized entities. More specially, the below three requirements can be further elaborated in WSNs as follows:

- Data Confidentiality

Confidentiality is required in sensors environment to protect information traveling among the sensor nodes of the network or between the sensors and the base station from disclosure. Confidentiality is an assurance of authorized access to information. In the context of networking, confidentiality means that the information about communications should be kept in secret from anyone without authorized access permission. In WSNs, data of interest, which may vary depending on different applications and usually appears as event reports sent by the sensing nodes from event happening area via multichip paths to the sink.

- Data Authenticity

Authenticity is an assurance of the identities of communicating nodes. Every node needs to know that a received packet comes from a real sender. Otherwise, the receiving node can be cheated into performing some wrong actions. Authentication in sensor networks is essential for each sensor node and base station to have the ability to verify that the data received was really sent by trusted sender or not. Data reports collected by WSNs are usually sensitive and even critical, such as in military applications. Hence, it is important to assure data authenticity in addition to confidentiality.

- Data Availability

Availability is an assurance of the ability to provide expected services as they are designed in advance. It is a very comprehensive concept in the sense that it is related to almost every aspect of a network. Any problem in a network can result in the degradation of the network functionality and thus compromise the network availability, leading to the DoS. As compromised nodes are assumed to be existing in WSNs, it is important to prevent or be tolerant to their interference as much as possible to protect data availability.

B. Security Threats InWsns

- In WSNs, the attacker could compromise multiple nodes to obtain their carried keying materials and control them .This type of attack could lead to severe data confidentiality compromise in WSNs.
- The attacker may use compromised nodes to inject bogus data traffic in WSNs. This type of attack could lead to severe both data authenticity and availability.
- Lastly, the attacker could also use compromised nodes to launch a selectiveforwarding attack, in which case compromised nodes selectively drop the going-through data traffic and, thus, data availability can be severely damaged.

IV. RELATED WORK

Wireless sensor network is used in a wide range of environments. They are vulnerable to more attacks than the conventional networks, due to the various inherent characteristics of wireless communication. Most critical is to achieve authentication and data confidentiality. Some of the papers reviewed to get an idea of the different systems existing in WSN are as follows:

A. An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks, 2004

S. Zhu, S. Setia, S. Jajodia, and P. Ning[3] proposed a scheme called interleaved hop-by-hop authentication (IHA) and is one of the first works in data authentication for wireless sensor networks. In this scheme, the sensor nodes are organized into clusters. The collaboration of a minimum number of nodes inside a cluster is generated a appropriate report. Every cluster has a representative that is called the cluster head (CH). The CH is responsible for collecting enough number of message authentication code (MAC) values generated by the collaborating nodes, generating a

report, and forwarding it to the sink. The forwarding path from every node to the sink is discovered at the initialization phase. The authenticity of the report is verified at every hop of the forwarding path to the sink by the aid of the MAC values. For this purpose, authentication chains are discovered and authentication keys are established both at the initialization phase of the network operation. A report with even one unverified MAC is regarded as bogus and dropped enroute. Therefore, a malicious node injecting noise to the network always causes these messages to be dropped. The other drawback of IHA is the association maintenance that introduces high communication overhead.

B. Statistical en-route filtering of injected false data in sensor networks, 2005

F. Ye, H. Luo, S. Lu, and L. Zhang[4] have proposed a Statistical En-route Filtering (SEF) mechanism that is very similar to IHA. The main difference is that associated nodes are not manually determined at the initialization phase. In contrast to IHA, the associated nodes are discovered by a probabilistic approach. In SEF, every node is pre-distributed with the keying material that are used to establish the authentication keys after the network deployment. The key pre-distribution parameters are selected to guarantee, with a high probability, that any CH is able to establish many authentication keys. The SEF provides data availability similar to IHA. Because of the probabilistic nature of SEF, every node is required to store many keys to guarantee the existence of a minimum number of authentication keys. Therefore, two other drawbacks of SEF are the requirement forlarge storage memory and the possibility of revealing many authentication keys by compromising only a few nodes.

C. Toward resilient security in wireless sensor networks, 2005

H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh[6] employed to achieve graceful performance degradation to an increasing number of compromised keys, the location-binding keys and location-based key assignment than both previous schemes (IHA and SEF) have a threshold property, i.e., an adversary has to compromise a minimum number of authentication keys to forge a report. The proposed scheme, called location-based resilient security (LBRS), is conceptually very similar to the SEF. However, the data is forwarded toward the sink in a hop-by-hop fashion. Thus, LBRS localizes the adversarial activities to only the area of the network which is under attack. The LBRS inherits the disadvantages of the SEF except the performance degradation behavior.

Existing security designs provide a hop-by-hop security paradigm only, which leaves the end-to-end data security at high stake. Data confidentiality and authenticity is highly vulnerable to insider attacks, and the multihop transmission of messages aggravates the situation. Moreover, data availability is not sufficiently addressed in existing security designs, many of which are highly vulnerable to many types of Denial of Service (DoS) attacks.

V. END-TO END VERSUS HOP-BY-HOP DESIGN

Recent research has seen a growing body of work on security designs for WSNs [3], [4], [6], [8], [9]. Due to the resource constraint, most of the proposals are based on symmetric cryptography and only provide data authenticity and/or confidentiality in a hop-by-hop manner. End-to-end encryption/ authentication is considered less feasible, particularly in a WSN consisting of a large number of nodes. However, lack of the end-to-end security guarantee could make WSNs particularly vulnerable to the aforementioned attacks in many applications where node-to-sink communication is the dominant communication pattern. This could give the attacker the advantage to obtain/ manipulate its desired data using much less effort without having to compromise a large number of nodes. To make things worse, existing security designs are highly vulnerable to many types of Denial of Service (DoS) attacks such as report disruption attacks and selective forwarding attacks.

In the past few years, many secret key pre-distribution schemes have been proposed [2], [8], [9], [10]. By leveraging preloaded keying materials on each sensor node, these schemes Two types of node compromise are considered: random node capture and selective node capture, according to key distribution. Hop-by-hop security design works fine when assuming an uniform wireless communication pattern in WSNs. However, in many applications node-to-sink communication is the dominant communication pattern in WSNs, that is, data of interest are usually generated from the event happening area and transmitted all the way to the sink. In this case, hop-by-hop security design is not sufficient any more as it is vulnerable to communication pattern oriented node capture attacks. Data confidentiality can be easily compromised due to lack of end-to-end security guarantee, since compromising any intermediate node will lead to exposure of the transmitted data. At the mean time, as the attacker could decrypt the intercepted data, it could therefore, freely manipulate them to deceive the sink and hence, severely affects data availability. The lack of end-to-end security association also makes it hard, if not impossible at all, to enforce data authenticity. We therefore conclude that end-to-end security design is much more desirable for WSNs as compared to hop-by-hop design when node-to-sink communication is the

dominant communication pattern as it can offer a much higher security resilience.

VI. PROBLEM STATEMENT

A. *System model*

Wireless sensor nodes may be deployed into some target field to detect the events occurring within the field. For example, in a military application, they may be deployed to a battlefield to detect the activities of enemy forces. We assume that sensor nodes form a number of clusters after deployment, each containing at least *n* nodes. In each cluster, one node is randomly selected as the *cluster-head*. To balance energy consumption, all nodes within a cluster take turns to serve as the cluster-head. That means physically there is no difference between a cluster-head and a normal node because the cluster-head performs the same sensing job as the normal node.

Fig.3.illustrates the organization of sensing nodes in wireless sensor networks. In the figure *CH* and *BS* denote *Cluster-Head* and *Base Station* respectively. *u1~u5* are forwarding are forwarding nodes, and *v1~v8* are sensing nodes (they can also serve as the forwarding nodes for other clusters). The black dots represent the compromised nodes, which are located either in the clusters or en-route.

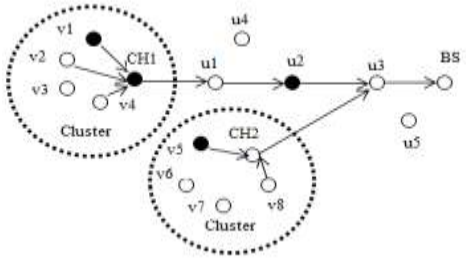

Fig. 3. Sensor nodes are organized into clusters. The big dashed circles outline the regions of clusters.

VII. SIMULATION AND RESULTS

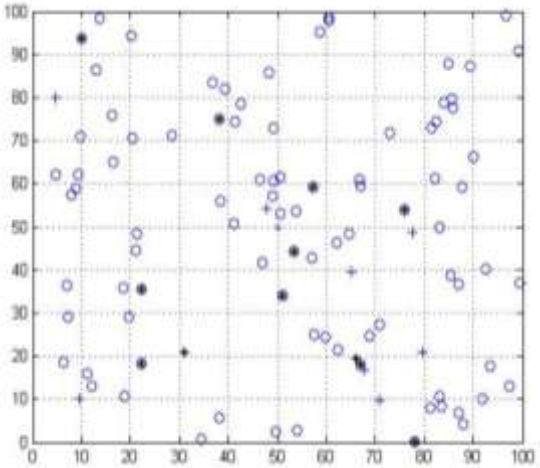

Fig. 4.Randomly distributed nodes.

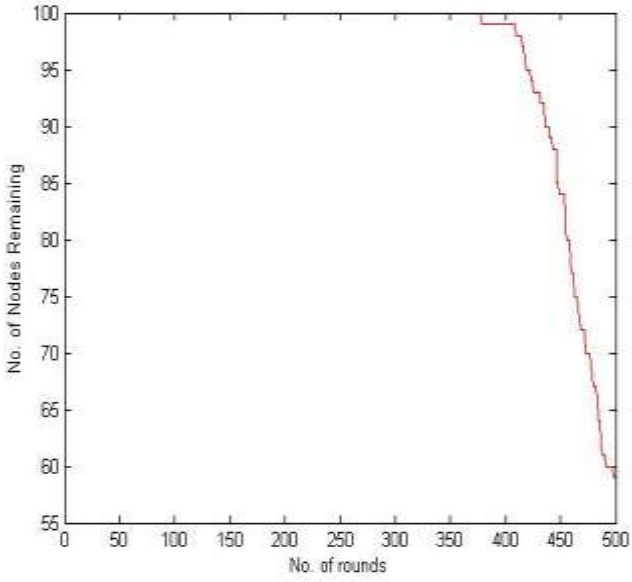

Fig. 5. The network lifetime

REFERENCES

[1] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, pp. 103-105, Oct. 2003.

[2] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc.IEEE Symposium Research inSecurity and Privacy",May 2003.

[3] S. Zhu, S.Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-By-Hop Authentication Scheme for Filteringof Injected False Data in Sensor Networks".Proc. IEEE Symp. Security and Privacy, May 2004.

[4] F. Ye, H. Luo, S. Lu, and L. Zhang, "Stastical En-Route Filtering of Injected False Data in Sensor Networks," In IEEE INFOCOM'04, Hong Kong, China, Mar. 2004.

[5] A. Wood and J. Stankovic, " Denial of service in sensor networks", IEEE Computer Magazine, vol. 35, no. 10, Oct. 2002

[6] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, " Toward Resilient Security in Wireless Sensor Networks," in Proc. ACM Int. Symp. Mobile Ad Hoc Net. Comput-MobiHoc, 2005.

[7] W. Du, J. Deng, Y. Han, and P. Varshney, "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," ACM Trans. Information and System Security, vol. 8, no. 2, pp. 228-258, May 2005.

[8] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A Key Management Scheme for Wireless SensorNetworks Using Deployment Knowledge," IEEE Trans.Dependable and Secure computing, vol. 3, no. 2, pp. 62-77, Jan-Mar. 2006.

[9] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing Pair-Wise Keys for Secure Communication in Ad HocNetworks: A Probabilistic Approach," Proc. IEEE Int'l Conf.Network Protocols (ICNP'03), Nov. 2003.

[10] L. Eschenauer and V. Gligor, "A Key-Management Scheme for Distributed Sensor Networks", In ACM CCS, Washington, DC, Nov. 2002.