SPSF: Server Predominant Security Framework for Wireless Sensor Network in Mission-Critical Applications

Liu Qiang, Cui Yimin, Kuang Xiaohui, Liu Li, Sun Xiaoxia
National Key Laboratory of Science and Technology on Information System Security
Anxiang Beili 10#, Chaoyang District, Beijing
CHINA
Liuqiang_xjtu@163.com

Abstract: -We focus on the security of *Wireless Sensor Network* (WSN) in mission-critical applications, which imply that the WSN may be deployed in untrusted or hostile circumstances, and once its security is compromised, the result is disastrous. So, the security should be taken seriously and given priority in the design of WSN in mission-critical applications. In this paper, we propose a *Server Predominant Security Framework* (SPSF), which emphasizes utilizing the advantages of resources and whole network's situation in the server side, and coordinating the secure efforts of both the server and the sensor nodes. Based on our framework, this paper presents a *Server Predominant Routing* (SPR) and discusses its security mechanisms. SPSF is a framework of distributed information gathering and centralized decision making for WSNs in mission-critical applications. SPR is a novel routing method based on SPSF and helpful to integrate various security mechanisms for satisfying the essential security demands for WSN in mission-critical applications.

Key-Words: - Wireless sensor network; security framework; secure routing

1 Introduction

Wireless sensor network (WSN) is composed of hundreds of inexpensive sensing devices with computational and communication resources, and provides a useful interface between the real world and the human with their data acquisition and processing capabilities. Sensor nodes are densely deployed either very near or inside the objects to be observed. WSNs have become the ideal instruments to monitor the environment in a variety of applications such as river pollutants detection, forest fire monitoring, military surveillance, etc. and their applications are continuously growing in popularity.

However, the major problem that hinders the applications of WSN is the lack of security of its nodes and communication. No doubt, the information infrastructures, which depend on a WSN without security assurance, may lead to disasters.

Basically, the security requirements of WSN are application dependent. Although many studies have been done, the security problem is still the crucial factory of restricting to apply WSN in mission critical applications. The alteration of the situation to promote the WSN applying to mission critical applications may face the following challenges:

- Once the sensor networks are applied to the mission-critical tasks, security should be taken into account in the design phase. But the current major protocols and its implements for WSN are demonstrated insecure [1].
- Resource constraints on the sensor node and the communication restrict the designer from appending security measures at will.

Our focus is on the security of WSN in mission-critical applications, such as traffic regulation, smart mine system, battlefield surveillance, etc. Compared to the usage in the application of the room temperature acquisition, the application of the WSNs in the remote surveillance has some characters close related to the security demands analysis:

- Be applied to mission-critical task.
- Be placed in untrusted or hostile circumstance, facing malicious attacks.
- Resulting in failure or disastrous once its security is compromised.

In this paper, the attacks against WSN are reviewed firstly, and we analyze the essential security demands for WSN in mission-critical applications. Then, we propose our novel framework, which emphasizes to coordinate the secure efforts of both the server and the

sensor nodes. Thirdly, we present a novel routing method based on our framework and discuss its security in detail. The last section is the conclusion.

2 Problem Formulation

Security issue of WSN is a hot topic in recent years. Researches have presented almost similar conclusions on types and mechanisms of attacks against WSN and relative security countermeasures. However, the possible presence of laptop-class adversaries and insiders and the limited applicability of end-to-end security mechanisms make the security design of WSN more challenging. Mission-critical applications require the WSNs have the abilities to resist various threatens and keep trustworthy. There is a big gap between the situations of the nodes left unattended in the hostile environment and the security requirements of mission-critical applications.

2.1 Attacks

Karlof and Wagner gave the first comprehensive analysis of secure routing in sensor networks [1]. They presented how attacks against sensor networks and introduced two classes of novel attacks against sensor networks. They described crippling attacks against the major sensor network routing protocols and suggested countermeasures and design considerations. Padmavathi etc. summarized a wide variety of attacks and different available mechanisms to handle them [2]. T. Giannetsos and T. Dimitriou demonstrated Spy-Sense, a spyware tool that allows the injection of stealthy exploits in the nodes of a sensor network [3]. Table 1 summarizes the relevant attacks against WSN.

Table 1 Summary of attacks against WSN

Type	**Relevant attacks**	
Active attacks against communications	Application layer	Fake ,evil data, etc.
	Transport layer	Flooding, replay attack, etc.
	Network layer	Sybil, wormholes, sink-hole, acknowledgement spoofing, selective forwarding, etc.
	Data link layer	Channel collisions attack
	Physical layer	radio jam attack
Passive attacks against communications	Radio sniffer, flow analysis, packet crack, etc.	
Active attacks against nodes	Inject, replication, disassembly, destroy, etc.	

Experts in network and cryptographists have provided a lot of custom-built algorithms for WSN, to prevent unauthorized people from reading and altering messages on a WSN. Many researches on mechanisms of secure routing and key management are proposed [1], [4-7], [8-12].

2.2 Security demands

When we talk about security of WSN, we should first apply the "need to know" principle, i.e. which security properties should be provided for WSN design. Bishop gave the concept of Computer security, which rested on confidentiality, integrity, and availability [19]. Many security researches on WSN have given a series of descriptions [1], [2], [4], [5], [15-17]. Several security requirements are summarized as follows:

- Confidentiality. Confidentiality is the concealment of information or resources. Information must be protected from disclosure to authorized parties.
- Integrity. Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity provides the ability to ensure that any changes in the message are easy to detect.
- Authenticity. Authentication is used to identify the sender of the message precisely.
- Availability. Availability refers to the ability to use the information or resource desired.
- Freshness. Freshness refers to the data is fresh and need the real-time requirement of the application.

As a goal of the design for mission-critical WSN, the designer should guarantee the contents of any message should not be inferred and satisfy the above requirements even in the presence of resourceful adversaries.

The physical and MAC layers are susceptible to direct attacks. Adversaries can jam radio links by radio jam attack and channel collisions attack. The design or the choice of radio platforms are not discussed in this paper.

As for outsider adversaries, link layer security mechanisms can guarantee integrity, authenticity, and confidentiality of messages because they deny an outsider access to the network. TinySec provides such a link layer security mechanism for WSN [13], and its

ISBN: 978-1-61804-134-0

implementation has been incorporated into the official TinyOS release [14].

The presence of insider attacks significantly weakens the effectiveness of link layer security mechanism and cryptography mechanism. Because a compromised node has complete access to any messages routed through it and is free to modify, suppress, or eavesdrop on the contents. So, security against insider attacks must be considered in the design.

Therefore, as for the WSN in mission-critical applications, the design must especially satisfy the following security requirements in addition:

- The security design must provide the ability to ensure or judge the trustworthiness of data. For example, in the scenario of remote surveillance, it is vital that the information is convinced of the trustworthiness of the data received.
- If the attack from compromised or insider attackers is inevitable, especially those with laptop-class capabilities, the security design must provide the ability to support a series of valid and rapid responses to prevent further attacks based on the compromised nodes.
- Communication should keep confidential, especially in the procedure of key negotiation.

3 design overview

In this section, we present a novel framework for WSN in mission-critical applications. We begin with the description of the WSN network model in mission critical applications. We then discuss the reasons and benefits of incorporating the server to build the trust architecture. The third subsection shows our framework.

3.1 Network model

Consider the scenario of remote surveillance WSN, we give some assumptions below:

- The nodes are randomly distributed within the limited areas.
- The nodes are immobile. Each of them equips a GPS module, which provides the location service on demand, and turns off in order to save power.
- Once deployed, the nodes are immobile and self-organize to build a network.

As shown in Fig. 1, for the sake of supporting large-scale WSN, we choose the physical location based clustered architecture to describe the topology of the WSN for mission-critical applications. Base station is typically a gateway to another network, which has sufficient power and bandwidth for communication. The messages are transferred in multi-hop between the sensor node and the server. The server is the interface between the net and the application system, which allow users to get information on the remote battlefield. Although the node has no mobility, the topology will change with the transition of node states.

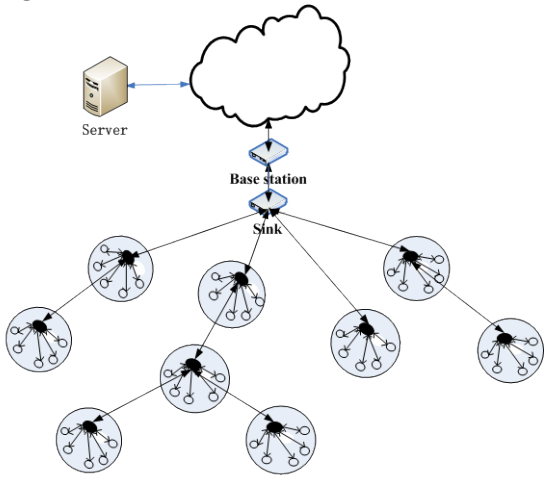

Fig. 1 A representative WSN architecture in mission-critical applications

3.2 Motivation

According to the discussion on security demands in subsection 2.2, the design for WSN in mission-critical applications should pay more attention to the insider attackers, especially the laptop-class adversaries.

Reputation and trust are very useful means and used to facilitate decision making in diverse fields, and recently have been adapted to WSNs. Existing reputation-based systems, such as confidant and RFSN, nodes maintain reputation for other nodes and use it to evaluate their trustworthiness [20-23]. Based on the mechanism of reputation and trust, a node can determine whether other nodes have been compromised, and take correct actions, through negative information sharing and independent trust-based decision making. But there are some problems which need to be resolved:

- The users in server side are not capable of estimating the trustworthiness of the data received.
- The mechanism of a node determining whether other nodes have been compromised makes the system vulnerable to false report attacks.

ISBN: 978-1-61804-134-0

- Existing frameworks lack adequate flexibility of responding to the attacks against WSNs in real mission-critical applications.
- Real embedded system could not suitable for using highly sophisticated arithmetic and saving large amount of history data, because of the resource constraints of sensor node.

Our intent is to design a framework for mission-critical WSN, in which the server is in charge of coordinating the security and the communication. Getting the server to participate in the management of the security and the communication has some obvious benefits:

- The server has the enough resources advantage. In addition, in the server side there are valuable assists from specialist and data obtained from the other intelligence information sources.
- Compared with the wireless sensor nodes deploying in unattended and hostile environment, the server itself is under the control and trust.
- Mission-critical application needs the ability of judging the trustworthiness of data received. Meanwhile, the user in the server side needs a way to flexibly operate and control the network according to security requirements and policies.

3.3 Framework

Fig. 2 shows our framework of security for WSN in mission-critical applications. Most activities of management and analysis are migrated into the server side, where the server has adequate resources and specialist assists. The node side provides the agent-based secure mechanism for supporting server predominant security service. We termed the framework as Server Predominant Security Framework (SPSF). The link layer security mechanisms are adopted to avoid outside attacks.

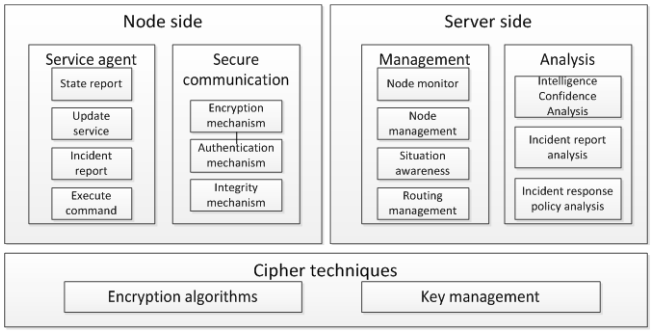

Fig. 2 Server Predominant Security Framework for mission-critical WSN

On every node is running a service agent, which is the bridge for reporting and receiving management messages between itself and the server. The interactive primitive types between the nodes and the server are summarized as table 2.

Table 2 Interaction primitive types in SPSF

Direction	Type	Object (message)
Node→ Server (up)	Report	The coming state changing
		The state changed
		The security event
		The alarm on abnormality of neighbourhood
	Reply	The state information which the server inquired, such as location, power, statistics, etc.
		The execution result which the server demand
	Request	The scheduled service from the server
Server→ Node (down)	Inquire	The current state information of specific nodes
	Reply	The information which the node request.
	Dispatch	The patch data to specific nodes for update service
		The command to specific nodes
		The routing information

In order to avoid the false security message attacks, light-weight public key based signature and encryption mechanisms are adopted in our framework to provide secure communication.

Our integrated framework brings an evolution of making the mission-critical WSN measurable and controllable. In the mission-critical WSN applications, our server predominant security framework provides the foundation for users to attain the ability to monitor the nodes, the ability to influence routing paths, the ability to judge the confidence of the intelligence, the ability to response to incidents.

4 SPSF based routing

Based on our server predominant security framework shown in Fig. 2, we present a dual routing protocols pattern. A classic routing protocol is built in each node as the backup approach, such as flooding routing protocol or AVDO routing protocol. Our Server Predominant Routing (SPR) is adopted as the primary routing method.

4.1 Initiation of routing

Cryptography provides a mechanism for secure communication. The light-weight public key mechanism could adapt to the resource constraints of the sensor node. The server is trust, and all nodes can be treated as trusted nodes before deployment. Every node is pre-distributed its unique ID, private key, the shared key and the public key of the server. The server knows all the keys including the private key of each node. At the deployment time, nodes use shared key to encrypt the neighborhood discovery message. In general, it should take the experienced attackers at least ten seconds to crack the share key. So, we can assume that the procedures of cluster topology initiation and neighborhood discovery are secure. The share key will be no longer valid once the topology constructed.

The initialization procedure of routing establishment is based on the backup routing protocol at the same time. Once the routing is established, each node reports in detail its state to the server, such as position, power, neighbours, and so on. Light-weight public key based secure communication mechanism ensures integrity of the report message. The server may draw out the initial state of the net based on the reports from the valid nodes. Some nodes may become isolated or invalid due to the troubles in deployment, such as the minimum distance from their neighbour is out of the max distance of RF.

4.2 Server predominant routing

When the initiation of routing finished, the server has the initial state of each node and the global network. The server calculates the reasonable routing according to the algorithms or policies. Then, the server uses dispatch messages to transfer routing information to nodes in secure communication way. When the node receives the routing information of its next hop, he inserts the information into the route table, which will be taken as the primary path.

The server and the nodes cooperate to maintain the routing. When report messages are received from nodes, the server records the events, evaluates its influence and responses the events immediately if needed, including dispatching new calculated routing information to the relative nodes. When the node finds itself cannot receive the message response from the server after several attempts, it turns to path discovery using the backup routing protocol and reports the event of communication failure later.

As described above, the max advantage of server predominant routing is the utilization of the global information. Our routing mechanism unlikely produces loop path, and has the characteristics of location-aware, energy-aware, global optimization, configurable and flexibility. Dual routing protocols pattern brings the routing procedure more robust.

4.3 Secure routing

Fig.3 shows the security information flows of SPSF based coordination for secure routing. In server predominant routing, the server can dig out evil nodes from the events of security and network state according to the reputation mechanism and the security policies.

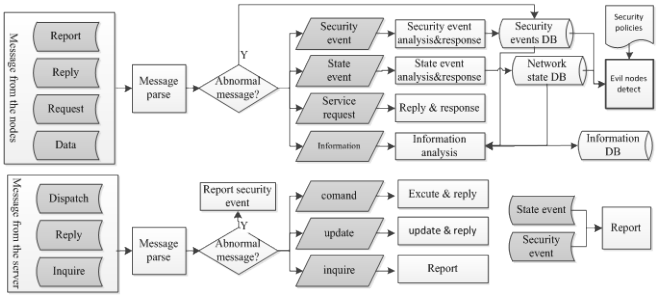

Fig. 3 SPSF based coordination for secure routing

As soon as the evil node is detected, the server can dispatch messages to alter the partial routing paths, and notify all neighborhoods to stop relay service for the evil node.

Based on our Server Predominant Security Framework, server predominant routing can also import heartbeat mechanism for link testing, time windows mechanism and challenge code mechanism in communication for avoiding replay attack, and so on.

5 Conclusion

In this paper, we propose a framework, SPSF, for developing a distributed information gathering and centralized decision making framework for WSNs in mission critical applications. Within the framework of SPSF, we present the server predominant routing, SPR, and show its security mechanisms. The framework and the routing are helpful to integrate various security mechanisms for satisfying the essential security demands for WSN in mission-critical applications. In the future, we will implement a prototype to verify its efficiency and security.

ISBN: 978-1-61804-134-0

References:

[1] Chris Karlof, David Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, *Ad Hoc Networks*, 1(2-3), 2003, pp. 293-315.

[2] G.Padmavathi, Shanmugapriya, A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Network, *International Journal of Computer Science and Information Security*, Vol.4, No.1&2, 2009.

[3] Thanassis Giannetsos, Tassos Dimitriou, Spy-Sense: Spyware Tool for executing Stealthy Exploits against Sensor Networks, *Black Hat, USA*, 2011.

[4] Yih Chun Hu, Adrian Perrig, A survey of secure wireless ad hoc routing, *IEEE Security and Privacy*, Vol.2, No.3, 2004, pp. 28-39.

[5] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru, and Herbert Rubens, An on-demand secure routing protocol resilient to byzantine failures, *Workshop on Wireless Security*, 2002, pp. 21-30.

[6] Jing Deng, Richard Han, and Shivakant Mishra, A performance evaluation of intrusion-tolerant routing in wireless sensor networks, *IPSN*, Springer, Vol.2634, 2003, pp. 349-364.

[7] Anthony D. Wood, Lei Fang, John A. Stankovic, and Tian He, Sigf: a family of configurable secure routing protocols for wireless sensor networks. *ACM SASN*, 2006, pp. 35-48.

[8] Laurent Eschenauer, Virgil D. Gligor, A key-management scheme for distributed sensor networks, *ACM Conference on Computer and Communications Security*, 2002, pp. 41-47.

[9] Qi Dong and Donggang Liu, Using auxiliary sensors for pairwise key establishment in WSN, *Lecture Notes in Computer Science*, Vol.4479 Springer, 2007, pp. 251-262.

[10] Donggang Liu, Peng Ning, and Rongfang Li, Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security*, Vol.8, No.1, 2005, pp. 41-77.

[11] Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, Jonathan Katz, and Aram Khalili, A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security*, Vol.8, No.2, 2005, pp. 228-258.

[12] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod K. Varshney, A key management scheme for wireless sensor networks using deployment knowledge, *INFOCOM*, 2004.

[13] Chris Karlof, Naveen Sastry, and David Wagner, Tinysec: a link layer security architecture for wireless sensor networks, *SenSys*, 2004, pp. 162-175.

[14] The TinyOS website, [Online], Available: http://www.tinyos.net

[15] Fei Hu and Neeraj K. Sharma, Security considerations in ad hoc sensor networks, *Ad Hoc Networks*, Vol.3, No.1, 2005, pp. 69-89.

[16] Sasha Slijepcevic, Miodrag Potkonjak, Vlasios Tsiatsis, Scott Zimbeck, and Mani B. Srivastava, on communication security in wireless ad-hoc sensor networks, *WETICE*, 2002, pp. 139-144.

[17] Adrian Perrig, John A. Stankovic, and David Wagner, Security in wireless sensor networks, *Comm.*, ACM, Vol.47, No.6, pp. 53-57.

[18] Naveen Sastry and David Wagner, Security considerations for IEEE 802.15.4 networks, pp. 32-42.

[19] Matt Bishop, Computer Security: Art and Science, Boston, USA, Addison Wesley, 2002.

[20] Buchegger S, Boudec J L, Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks, *the Tenth Euromicro Workshop on Parallel*, 2002, pp. 403-410.

[21] Ganeriwal S, Srivastava M B, Reputation-based Framework for High Integrity Sensor Networks, *the 2nd ACM workshop on Security of ad hoc and sensor networks*, 2004, pp. 66-77.

[22] Garth V. Crosby, Lance Hester, Niki Pissinou, Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks, *International Journal of Network Security*, Vol.12, No.2, pp. 107–117.

[23] S. Ganeriwal, M. Srivastava, Reputation-based framework for high integrity sensor networks, *the 2nd ACM workshop on Security of ad hoc and sensor networks*, 2004, pp. 66-77.