Security Issues and Challenges in Event-Driven Wireless Sensor Networks

Lulu Liang, Qi Zou, Guang Yang, Lei Shi
China Information Technology Security Evaluation Center
Beijing, 10085, P.R. China
E-mail: {liangll, zouq, yangguang, shilei}@itsec.gov.cn

***Abstract*—Recently, wireless sensor networks (WSNs) have attracted a lot of attention from the network research community, especially in the aspect of event-driven wireless sensor networks (EWSNs), such as adversary locating, fire detection and so on. As the nature of importance of event monitoring, security has to be assured in both of communication and processing. However, due to the inherent resource constraints, security in EWSNs is faced different issues and challenges than traditional WSNs. In this paper, we attempt to give an outline on the security issues in the EWSNs. And then we propose a new secure architecture for it, which covers potential security issues. In this architecture, we analyze the possible threats and give out the corresponding countermeasures.**

Keywords-security; threat; issue; event-driven wireless sensor networks

I. INTRODUCTION

Wireless sensor networks (WSNs) are consisted of a large amount of self-organizing, low-power, low cost wireless sensor nodes with constrained resources, deployed randomly or artificially for particular application. Due to the feature of low cost, it is possible to deploy large sensor arrays in different conditions to perform both military and civilian tasks [1]. In most of the applications, there is a clear difference between data *sources* and *sinks* where the data should be sent to. Depending on the interaction patterns between sources and sinks, these applications of wireless sensor networks can be categorized as follows [2]:

- **Event detection**: A large amount of sensor nodes are deployed to monitor a specified event. Once they have detected the event, sensor nodes will report the event information to sinks quickly. A simple event can be detected by a single sensor node with only one property, while a complex event (composite event [3][4], for instance) will be detected with the collaboration of nodes around the event area.
- **Periodical measurements:** The WSNs are tasked with periodically reporting measured values. Often, the reports are periodical and automatic, such as environment monitoring applications. However, sometimes, the reports can be triggered by a detected event and the reporting period is practical.
- **Function approximation and edge detection**: The alteration of a physical value like temperature changes from one place to another can be regarded as a function of location. We can extract its spatial characteristics by approximating this unknown function, using a limited number of samples. Similarly, with the help of WSNs we can find the isothermal points in a forest fire application to detect the border of the actual fire[5].
- **Target tracking:** In some applications, such as intrusion detection, the event may be mobile. The WSNs can be used to report the event information to sinks, potentially estimating about the speed, direction or other properties of event simultaneously. In this situation, sensor nodes may have to cooperate for making decision.

In these applications, we can find that most of applications are based on event detection, such as edge estimation and target tracking, which focus on helping to protect human life as well as valuable goods. Due to the importance of these systems, the sensor nodes must not be compromised by the intentional attacks, a reliable security system is very important. For the event monitoring applications, the character "reliable" means not only the secure communication but also the secure event detection.

Different from traditional wireless sensor networks, EWSNs have more stringent secure requirements. Taking the event detection for example, firstly we could not tolerate that the event information is tempered maliciously by intentional adversary. Secondly, we should try our best to deliver the event information to the sink nodes as reliable and fast as possible. However, the wireless medium in EWSNs is easily accessible by anyone and thus does not provide any protection against malicious adversaries. The adversaries can easily launch an eavesdropping or passive traffic analysis attack once connected to the network. Even more serious, the adversary could actively manipulate the network by removing, inserting or modifying the packets which contain important event information. Considering this, it is quite obvious that the EWSNs need a security environment to guarantee the reliable event monitoring. Recently, with the advent of real-world applications in the area of EWSNs, the need for applicable secure event detection and communications increasingly move into the attention of research.

However, the existing literatures focus on the traditional security problem in wireless sensor networks, such as cryptography, identity authentication, key management, trust management, access control, intrusion detection and so on. Most of the methods they proposed can only handle with single threat or few threats as they deal with the problems from the perspective of different attacks. In this paper, we analyze the security problem in EWSNs and propose a new secure architecture for EWSNs, which reduces the communication cost and saves energy. Based on this

Published by Atlantis Press, Paris, France.

architecture, we analyze the possible threats and give out the corresponding countermeasures.

II. HYBRID ARCHITECTURE OF EWSNS

Sensor nodes are very important components for event monitoring, while the particular sensor types vary significantly depending on the application. In the past decade, a number of sensor nodes have been developed to aid research. In general, the sensor nodes can be classified into *low-end* and *high-end* platforms based on both capability and usage.

***Low-end platforms*:** The low-end platforms [6][7] are characterized by the limited capability in terms of processing, memory and communication bandwidth. These sensor nodes are usually equipped with low-power processor and transceiver to decrease the cost and energy consumption. Thus, often they are deployed in large numbers to accomplish sensing tasks cooperatively through multi-hop communication.

High-end platforms: Compared with low-end platforms, high-end platforms [8][9] are equipped with higher processing capability and memory space. Practically, we need not only large amount of low-cost sensor nodes to sensing but also the high-end platforms to accomplish high-level tasks such as key distribution, data aggregation, network management and so on. Besides, with the help of high-end platforms, WSNs can be integrated into existing infrastructure more conveniently.

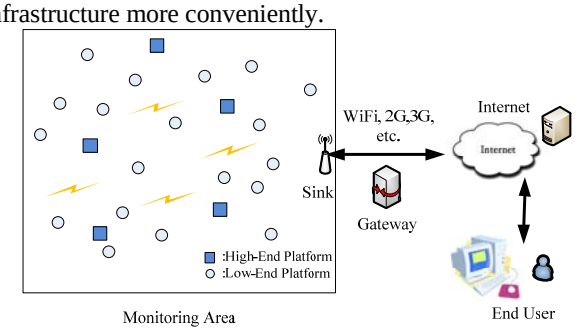

Figure 1. The architecture of EWSNs

Based on the low-end platforms and high-end platforms, the architecture of EWSNs is shown in

Figure 1. A large amount of sensor nodes are deployed randomly or artificially in the target zone to accomplish the event monitoring tasks. As soon as the specified event occurs, sensor nodes around the event will sense this phenomenon and transmit it to sink node through multihop communication. And then, the event information will be delivered to the internet through gateway. Remote user could easily obtain the information for further decision timely.

III. DISTRIBUTED EVENT DETECTION

In this paper, we propose a new architecture for distributed event detection (Figure 2), where each immediate node could make final decision at the delivery process. It combines the advantages of architecture in the first case and second case. Firstly, each sensor node i could make local decision u_i with the raw sample data y_i like the first case. And then each node i transmits the local decision u_i to sink node. The innovation is that each forwarding node j could make the final decision as long as receiving enough information. The importance is that we do not need the sampled values of each node any more, but only m ($m<n$) values are enough, such as the sequential detection method [10]. The worst case in this architecture is that it is still the sink node which makes final decision. In this architecture, we could get rather high detection accuracy at the lower cost energy consumption.

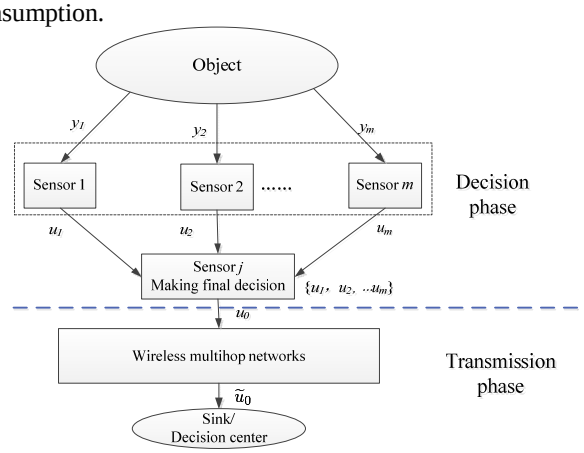

Figure 2. Distributed event detection

In this architecture, event detection is divided into two phase, decision phase and transmission phase, as shown in Figure 2. In the decision phase, each sensor node senses the environment and sends the sampled value to sink node. Any immediate node forwarding the sensed message could make the final decision as soon as receiving enough information. The most importance of this phase is obtaining a final decision u_0. However, the decision process is still under study, which is still a very complex and challenging problem.

And then, we will send the final decision information u_0 to the sink node, which is in transmission phase. Different from other packets, we have to assure the transmission probability of the final decision u_0 at a very high level, even nearly 100%. The reliable transmission of final decision is correlated with many aspects, congestion, wireless channel interruption and so on. Until now, There are many literatures about the reliable transmission [11][12][13]. However, most of them assume that sensor nodes are trustworthy and there are no any attacks in networks. How to transmit the critical packets with high quality of service requirements at a low cost is a very challenging work in the future.

IV. SECURITY ISSUES IN EWSNS

As the wireless communication is insecure and easily susceptible to various attacks, in addition to the limited resource characteristics, EWSNs are facing more serious secure issues than traditional wireless networks. There are number of different threats to the EWSNs like Denial of Service (DoS), Jamming, Eavesdropping, tempering, etc. Usually, a sensor node is equipped with limited communication and computing devices, which are more vulnerable to various attacks. Thus, in a large-scale sensor

networks, it is challenging to monitor and protect each individual sensor node from attacks and misbehavior.

Based on the capability of attacker, treats can be categorized into sensor-level and laptop-level. Obviously, a powerful laptop-level attacker with larger computation and communication capability will do much more harm to the network than a sensor-level attacker. Based on the boundary of attacker, the threats can be classified into outside and inside ones. An inside attacker has trusts of other nodes and is much harder to defend against.

Recently, there are many articles in the literatures dealing with different threats in WSNs, such as [14][15]. They have analyzed many types of attacks and given an overview of the possible defense methods. In this paper, we focus on the negative effect on event detection of different threats from the perspective of network layer [16][17][18].

A. Physical layer

Most of the physical layer attacks are attempting to prevent the wireless communication by disturbing the radio or tampering the packets.

Jamming is a simple attack in physical layer, in which the adversary disrupts the operation of the network by broadcasting a high-energy signal. In EWSNs, most sensor nodes are equipped with low-cost transceiver. Taking CC2420 for example, the transmit power can be programmed from -15 to 0 dBm in 8 steps [19]. Thus, launching a Jamming attack is very easy and hard to defend against. As a variant of jamming attack, in *radio interference* attack, adversary produces the interference signal randomly or regularly. We could use frequency hopping or code spreading [20] to defend against it. However, it is too complex and expensive for low-end platforms. If the influence of interference source is a small region, another approach is to identify the jammed region and avoid it by designing an appropriate routing protocol [20].

Tampering is another important attack in which adversary can extract key information from the comprised nodes and then temper with its circuitry or even reprogram the codes. Preventing the adversary from comprising nodes is a complex problem. We may use self-destruction to avoid the information tampering.

B. Link layer

Link layer is responsible for data frame detection, medium access control and error control. Attacks at this layer are mainly focus on the medium resource assignment.

Collision is common in wireless communication, which occurs when two nodes transmit on the same frequency simultaneously. An adversary may launch a *collision* attack by transmitting packets strategically in an attempt to generate collision. When collision occurs, nodes have to retransmit the packets and consume extra energy. The continuous retransmission caused by the repeated collision can also result in *energy exhaustion*. Except for the waste of energy, the collision can also lead into *unfairness* if the adversary intermittently launches collision attack. This kind of attack is a weak form of DoS attack.

A possible defense against the *collision* attack is the use of error correction code (ECC) [20]. However, these introduced codes bring additional processing and communication overhead. Another typical countermeasure for *energy exhaustion* is using rate limiting MAC protocol or time-division multiplexing scheme. This scheme can solve the postponement problem caused by retransmission.

C. Network layer

Network layer of EWSNs is most vulnerable to different types of threats. As the complexity of network protocol, the types of attacks are also diverse and hard to defend against.

Routing protocol is one of the most important components of network layer. Many adversaries pay great attention on the routing protocol by various attacks to disrupt the routing and communication. Hello packets are required in many routing protocols to establish the neighbor relationship. A laptop level attacker many send similar hello packet to other remote sensor nodes to change to network topology. Besides, each node receiving the hello packet firstly may forward it, which result in *Hello Flood* attack. Another direct attack against the routing protocol is to spoof, alter or relay the routing information to disrupt communication in network, namely *spoofing* attack. A possible defend against this attack is using a message authentication code at the end of packet, in which the receiver can verify the consistency and integrity.

Forwarding is a fundamental function at network layer. Some adversaries may launch *gray/black hole* attack by comprising sensor nodes. The comprised node may refuse to forward partial (*gray hole*) or whole (*black hole*) packets received and drop them. *Black hole* attack is easy to be detected and sensor node could attempt to select another next hop to forward packets. However, *gray hole* attack forwarding packets selectively can forward the other packets normally and reduce the suspicion. To overcome it, we could design multipath routing protocol combining with random or opportunistic routing to sink node.

As a more pernicious attack, *sink hole* attack could attract nearly all the packets around the malicious sensor node, like a sink hole with the attacker at the center. First of all, *sink hole* attack may create a comprised node looking more attractive to surrounding node. For example, the comprised node may announce that it has a high quality route path to sink node, by *spoofing* the routing information. Sink hole attack can result in many other attack, such as gray/black hole attack, spoofing attack and so on. We could use cryptography and authentication topology to avoid this type of attack.

Sybil attack poses a significant threat on the event detection sensor networks, in which, a single malicious node could present multiple nodes logically in networks by announcing different identities. In the decision phase (Figure 2), the final decision process is in fact a kind of data aggregation. The malicious node could pollute the aggregation result by injecting different primary packets. This attack will reduce the even detection accuracy greatly. Besides, sybil attack can reduce the effectiveness of geographical routing protocols. The malicious node can

spoof the topology information and then the location ware routing protocols will not work well again. A possible countermeasure against sybil attack is using shared random cryptographic techniques [21]. Initially, each node computes the common key which is used as the secret keys to ensure the hop-by-hop security.

Wormhole attack is another severe threat against data communication in sensor networks that is particularly challenging to detect and defend. In a wormhole attack, an attacker receiving a serial of packets at one point tunnels the packets received into networks to another point through a path like a wormhole and then relays them again[22]. Wormhole attack is normal in wireless networks due to the nature of wireless channel. It can also be used as a tool to launch sinkhole attack, in combination with gray or black hole attack. In [23],Y. Hu proposed a novel scheme called *packet leashes* to defend against the wormhole attack. Direction antenna technology can also be used to combat wormhole attack [25].

D. Transport layer

In fact, there is no explicit transport layer in EWSNs. If TCP/IP is adopted as the network protocol, such as Contiki OS [23], TCP or UDP is used as the transport layer protocol. Traditional attacks on wire networks for TCP/UDP is still useful, even worse, the attack may be easier.

Rude connection is a typical attack at transport layer, in which the adversary associates new connection request to target node continuously until its resource is exhausted. A possible approach against this attack is that the node associating each connection should demonstrate its commitment to the connection.

In some reliable transport protocol, the sender should retransmit the packet as long as detecting the packet loss, such as the intermittent sequence number. The adversary may continuously create messages to the nodes with retransmission request. Therefore, the packets will be retransmitted again wasting large amount of energy, resulting in the *de-synchronization* between sender and receiver. To defend against *de-synchronization* attack, authentication of header of full packet is required.

E. Application layer

At application layer, an adversary may attempt to inject large amount of useless packets into networks to overwhelm the networks, exhausting network bandwidth and energy. Besides, the injection action could also be generated by the network itself. Especially in EWSNs, the adversary may forge a virtual event with sensor stimuli, and then this stimulation will overwhelm the networks again. We can mitigate this attack by carefully setting the parameters so that only the desired stimulus can trigger the event. Of cause, we could use the cryptographic and authentication technologies to prevent the illegal packets.

V. OTHER SECURITY SCHEMES

The threats and countermeasures introduced above can effectively prevent sensor networks against some attacks. However, if the attacker is strong enough, all the protection schemes will not work well again. As the resource constraints, sensor nodes usually cannot deal with such strong adversaries. Authentication and cryptographic technology are also not enough for ensuring the network security.

An *intrusion detection system* (IDS) which monitors the networks for suspicious activity patterns is needed to detect the intrusion and exploit the insecurities. In wired networks, IDS provides an in-depth protection. However, little research has been performed in the area of wireless sensor networks. In WSNs, the IDSs are mainly classified into rule-based and anomaly-based systems [26]. The rule-based IDS is used to detect know attacks of intrusion [27], while anomaly-based IDS is used to detect unknown intrusion [28]. If most of the treats are known, a rule-based IDS outperforms anomaly-based IDS in term of the false-alarm rate. On the contrary, if most of the threats are unknown, an anomaly-based IDS outperforms rule-based IDS in term of the intrusion-detection rate. However, in EWSNs, sensor nodes are lack of resources in term of energy, memory spaces, and so forth. It is impractical to preinstall all the possible countermeasures against attacks before they are deployed. Thus, designing a light weight and effective IDS is quite challenging in wireless sensor networks.

Trust management is another approach for enforcing high-level of security in EWSNs. With the trust management, sensor nodes can establish a network with an acceptable level of trust relationships among themselves. Using the trust relationships, we can deal with many problems, such as intrusion detection, authentication, access control, and so on. However, most of the trust management schemes are designed for wireless ad hoc networks, such as [29][30], which are not suitable in EWSNs. In [31], S. Ganeriwal et al proposed a reputation-based framework in which a beta distribution for reputation representation, updates, and integration is employed. In [32], a comprehensive analytical and inference model of trust has been proposed. As the memory space is serious limited for storing trust related information of sensor networks, it is better to treat the nodes with equal weight and compute the average as the final trust. However, trust-based models often brings high computational and storage overhead. Building an efficient scheme is also a very challenging task for the resource constrained sensor networks.

VI. CONCLUSION

As the nature of vulnerability of wireless channel, security is a considerable critical issue wireless sensor networks. However, many protocols designed for EWSNs have not taken security into consideration. Especially in EWSNs, the security is particularly important as the particular task. In this paper, first we make a short survey about the current projects on the event monitoring applications. And then, we analyze the different security problem in EWSNs. Third, we proposed a novel event detection architecture for EWSNs. At last, we analyze the possible threats and give out the corresponding countermeasures from the perspective of network layer. Nowadays, the threats are more and more complex. However,

current studies on security in WSNs focus on the individual problem such as secure routing, key management and so on. Therefore, we had better consider the security problem systematically. How to design a light weight and energy efficient protocol to guarantee the wireless sensor networks is still a challenging work in the future.

REFERENCES

[1] J. Yick, B. Mukherjee, D. Ghosal. Wireless sensor network survey. Computer Networks, 52(12):2292-2330, 2008. ISSN 1389-1286.

[2] H. Karl, A. Willig. Protocols and Arhitectures for Wireless Sensor Networks. John Wiley & Sons Ltd, 2005.

[3] L. Liang, D. Gao, H. Zhang, and Oliver W. W. Yang. Efficient Event Detecting Protocol in Event-driven Wireless Sensor Networks. IEEE Sensors Journal, vol. 12, no. 6, pp. 2328-2337, June, 2012.

[4] Y. S. Li, C. Y. Ai, C. T. Vu, Y. Pan, and R. Beyah, "Delay-bounded and energy-efficient composite event monitoring in heterogeneous wireless sensor networks," IEEE Transaction on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1373–1385, Sep. 2010.

[5] D. Ganesan, D. Estrin, and J. Heidemann. DIMENSIONS: Why do we need a New Data Handling Architecture for Sensor Networks. ACM SIGCOMM Computer Communication Review, 33(1): 143–148,2003.

[6] Crossbow technology. http://www.xbow.com.

[7] Waspmote. Libelium opens access to bluetooth wireless sensor networks.http:// www.libelium.com.

[8] The Stargate platform.
http://bullseye.xbow.com:81/Products/productdetails.aspx?sid=229

[9] Sun Microsystems, Inc. Sun spot world. http://sunspotworld.com/.

[10] L. Yu and A. Ephremides. Detection performance and energy efficiency of sequential detection in a sensor network. in Proc. of HICSS'06, Hawai, USA.

[11] H.-X. Tan, M.-C. Chan, W. Xiao, P.-Y. Kong, and C.-K. Tham. Information quality aware routing in event-driven sensor networks. in Proc. IEEE INFOCOM, 2010, 1-9.

[12] V. C. Gungor, O. B. Akan, and I. F. Akyildiz. A real-time and reliable transport protocol for wireless sensor and actor networks. IEEE/ACM Transactions on Networking,16(2):359–370, April 2008.

[13] L. Liang, D. Gao, H. Zhang, Victor C.M. Leung. A Novel Reliable Transmission Protocol for Urgent Information in Wireless Sensor Networks. in Proc. IEEE GLOBECOM'10, Miami, FL, USA, 2010, 1-6.

[14] Y. Zhou, Y. Fang, Y. Zhang. Securing wireless sensor networks: a survey. IEEE communications surverys, vol. 10, no. 3, pp. 6-28, 3rd Quarter 2008.

[15] M. K. Jain. Wireless Sensor Networks: Security Issues and Challenges. International Journal of Computer and Information Technology, Vol. 2, no.1, pp. 62-67, 2011.

[16] Mohit Saxena, "Security In Wireless Sensor Networks - A Layer Based Classification", Cerias Tech Report 2007-04.

[17] T.Kavitha, D.Sridharan. Security Vulnerabilities In Wireless Sensor Networks: A Survey. Journal of Information Assurance and Security, pp. 31-44, 2010.

[18] Riaz A. Shaikh, Sungyoung Lee, Young Jae Song, Yonil Zhung, "Securing Distributed Wireless Sensor Networks: Issues and Guidelines", Proc. of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2006.

[19] CC2420. http://www.ti.com.cn/product/cn/cc2420?247SEM

[20] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", IEEE Computer, Vol. 35, No. 10, pp. 54-62, 2002.

[21] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks", In Proc. of the IEEE Symposium on Security and Privacy, pp.197, IEEE Computer Society, May 2003.

[22] Y.C. Hu, A. Perrig, D.B. Johnson, "Wormhole attacks in wireless networks", IEEE Journal on selected areas in communication, vol. 24, no. 2, pp. 370-380, Feb. 2006.

[23] Contiki OS. http://www.contiki-os.org/.

[24] Y. Hu, A. Perrig, and D.B. Jonson, "Packet leashes: A defense against worm-hole attacks", In Proc. of the 11th Annual Network and Distributed System Security Symposium, February 2004.

[25] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks", In Proceedings of the 11th Annual Network and Distributed System Security Symposium, February 2004.

[26] Y. Wang, G. Attebury, B. Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks" , IEEE Communications Surveys & Tutorials, Vol. 8, No. 2, 2nd Quarter 2006.

[27] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," Wireless Networks, vol.9, no. 5, 2003, pp. 545–56.

[28] Y. Huang and W. Lee, "Attack Analysis and Detection for AdHoc Routing Protocols," RAIS '04: Proc. 7th Int'l. Symp. Recent Advances Intrusion Detection, Sophia Antipolis, France, Sept.2004.

[29] A. Pirzada and C. McDonald, "Establishing trust in pure ad hoc networks", In Proceedings of the 27th Australian Conference on Computer Science, Dunedin, New Zealand, 2004, pp. 47-54.

[30] K. Ren, T. Li, Z. Wan, F. Bao, R.H. Deng, and K. Kim, "Highly reliable trust establishment scheme in ad hoc networks", Computer Networks: The International Journal of Computer and telecommunications Networking, Vol.45, pp.687-699, August 2004.

[31] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", In Proceedings of the 2nd ACM Workshop on Security on Ad Hoc and Sensor Networks, Washington DC, USA, 2004.

[32] Z. Liang and W. Shi, "Analysis of ratings on trust inference in the open environment", Technical report MIST-TR-2005-002, Department of computer Science, Wayne State University, February 2005.