Jyoti Panghal et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 3, Issue 2, June 2016, pp. 37-40

A Review on Security Analysis in WSN

Jyoti Panghal[1], Navneet Verma[2]

M.Tech Scholar, Geeta Engineering College, Panipat
Assistant Professor, Geeta Engineering College, Panipat

Abstract: In recent years, wireless sensor network (WSN) is employed in many application areas such as monitoring, tracking, and controlling. For many applications of WSN, security is an important requirement. However, security solutions in WSN differ from traditional networks due to resource limitation and computational constraints. This paper analyzes security solutions: TinySec, IEEE 802.15.4, SPINS, MiniSEC, LSec, LLSP, LISA, and LISP in WSN. This paper also presents characteristics, security requirements, attacks, encryption algorithms, and operation modes. This paper is considered to be useful for security designers in WSNs.

Keywords: WSN, Security threats

I. INTRODUCTION

Typically, WSNs contain a large number of sensor nodes, which are densely and randomly deployed in the field under study as shown in figure 1. Each of these scattered sensor nodesh as the capabilities to collect data and route data back to a collection point called a Sink. Data are forwarded to the Sink through a multihop wireless architecture as shown in figure1. Once the collected data reach the sink, it has to route them to the task manager, where the appropriate decisions can be made. The sink may communicate with the task manager node via Internet or satellite. The purpose of deploying a WSN is to report relevant data for processing which enables right decision making at the right moment. There are three types of reporting: event-driven, on-demand and continuous monitoring. In the event-driven reporting, the sensor network is tailored to detect the occurrence of a pre-specified type of event within the sensor field. Once this event occurs, the reporting task is initiated and the related information is forwarded to the Sink. Thus communication is triggered by the event occurrence and only nodes within the event area become sources of communication. The most famous detection based applications are: fire, food detection and alarms. In the on-demand reporting, communication is initiated by the Sink, and sensor nodes end their data in response to an explicit request. The important corresponding application is an inventory control system. One of the key features of a WSN is its multihop distributed operations, which add more complexity in terms of security attack detection and prevention. In a multihop distributed environment, it is very difficult to locate attackers or malicious nodes. Many security attack detection and prevention mechanisms are designed for WSNs; however most of the existing solutions are capable of handling only a few security attacks. For example, most secure routing protocols are designed to counter few security attacks.

Similarly new media access mechanisms are designed to handle hidden-node problem or selfishness. Encryption mechanisms are designed to protect data against passive attacks. Hence, one can say that there is a need to design mechanisms that are capable enough of detecting and preventing multiple security attacks in WSNs.

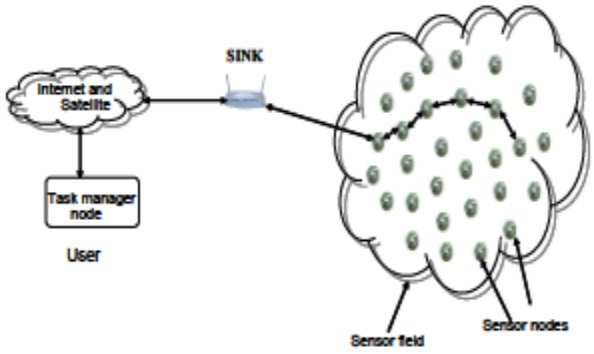

Figure 1: WSN design.

An Intrusion Detection System (IDS) is one possible solution to it. An intrusion is basically any sort of unlawful activity which is carried out by attackers to harm network resources or sensor nodes. An IDS is a mechanism to detect such unlawful or malicious activities. The primary functions of IDS are to monitor users' activities and network behaviour at different layers. A single perfect defence is neither feasible nor possible in wireless networks, as there always exist some architectural weaknesses, software bugs, or design flaws which may be compromised by intruders. The best practice to secure wireless networks is to implement multiline of security mechanisms; that is why IDS is more critical in wireless networks. It is viewed as a passive defense, as it is not intended to prevent attacks; instead it alerts network administrators about possible attacks well in time to stop or reduce the impact of the attack. The accuracy of intrusion detection is generally measured in terms of false positives (false alarms)and false negatives (attacks not detected), where the IDSs attempt to minimize both these terms. There are two important classes of IDSs. One is known as signature-based IDS, where the signatures of different security attacks are maintained in a database. This kind of IDS is effective against well-known security attacks. However, new attacks are difficult to be detected as their

signatures would not be present in the database. The second type is anomaly-based IDS. This kind is effective to detect new attacks; however it sometimes misses to detect well-known security attacks. The reason is that anomaly-based IDSs do not maintain any database, but they continuously monitor traffic patterns or system activities.IDS can operate in many modes, for example, standalone operation and cooperative cluster based operation. A standalone IDS operates on every node to detect unwanted activities. Cooperative cluster based IDS are mostly distributed in nature in which every node monitors its neighbours and surrounding nodes activities and operation; in case of any malicious activity detection, the cluster head is informed. Broadly speaking, IDS has three main components as:

i. Monitoring component is used for local events monitoring as well as neighbours monitoring. This component mostly monitors traffic patterns, internal events, and resource utilization.
ii. Analysis and detection module is the main component which is based on modelling algorithm. Network operations, behaviour, and activities are analyzed, and decisions are made to declare them as malicious or not.
iii. Alarm component is a response generating component, which generates an alarming case of detection of an intrusion.

II. PREVIOUS WORK

Intrusion detection system (IDS) is a system capable of detecting a range of intrusions and attacks. Dennig in [10] defined an intrusion detection model. Heady et al. in [11] designed a system monitoring a local network and capturing information about data packet transmission. The architecture of the IDS consisted of *data sampling and preprocessing* component and a *classifier system*. The data provided to the classifier system were following: packet size value, timestamp value and Ethernet source-destination ordered pair. The rule-based system could be run in either *learning process* or in a *decision process*. A *credit assignment algorithm* was used to assign a credit to the rules and a *genetic algorithm* was used to delete the rules or to generate new ones. Since that time, many intrusion detection systems have been developed for wired and also wireless networks. Zhang and Lee in [12] described vulnerabilities of ordinary ad hoc wireless networks and published their work on intrusion detection and response mechanism suitable for ordinary ad hoc wireless networks. They compared the ordinary ad hoc wireless networks with fixed wired networks and pointed out that the ad-hoc wireless networks did not have such concentration traffic point like routers, switches or gateways as the wired networks had. Hence, the only possible audit trace was limited to radio traffic and IDS techniques had to be based on some partial and localized information. They suggested that the IDSs suitable for ordinary ad hoc wireless networks should be *distributed* and *collaborative*. Pires et al. in [13] considered a solution for malicious node detection in WSNs based on the received signal strength.

Silva et al. in [14] proposed an IDS fitting the demands and requirements of WSNs. They claimed that the designer of an IDS should 1) select from the available set of rules those that can be used to monitor the desired features; 2) compare the information required by the selected rules with the information available in the target WSN to select final set of rules; and 3) set the parameters of the selected rules with the values of the design definitions. We believe that our proposed IDS framework will significantly help the network operators to follow this suggested process.

Classification

Techniques used in intrusion detection systems can be classified into two following categories :

- *Signature (misuse) detection.* Techniques based on signature detection are used to identify known intrusions. For example, they can analyze sniffed packets to find out whether they are malicious or not. The advantage is that the techniques based on signature detection can effectively and accurately detect known attacks. The disadvantage is that they cannot recognize novel attacks with unknown signatures.
- *Anomaly detection.* Techniques based on anomaly detection should be able to recognize unknown attacks because the traffic patterns can be compared with "training sets" characterizing normal behavior. If the traffic pattern deviates significantly, an intrusion is reported. The advantage is that the techniques based on anomaly detection do not require any prior knowledge of the attacks and can detect novel intrusions.

The disadvantage is that they can potentially cause high amount of false negatives or positives and cannot describe what kind of attack occurred. Providing a reliable training set may also be problematic.

Components and architecture

Silva et al. in [14] suggested to divide their algorithm for an intrusion detection system into three phases: 1) *data acquisition*, where packets are collected in a promiscuous mode and filtered before storage for further analysis; 2) *rule application*, where rules are applied on the stored data; and 3) *intrusion detection*, where the number of failures generated in the previous phase is compared to the number of occasionally expected number of failures to consider whether an intrusion occurred. Roman et al. in [15] pointed out that it is not possible to have an active intrusion detection agent in every node of a WSN because of limited battery capacity and proposed a general architecture for WSNs. They divided intrusion detection agents into two following classes:

i. *Local agents* monitor the activities performed on the node itself and on the sent or received packets. The agent only manages its own communication so the overhead is low.
ii. *Global agents* monitor the communication of its neighbors and analyze the content of the overheard packets. They can also be called *watchdogs*.

Only certain nodes in a WSN should usually be active agents at a time so as to conserve the energy and to prolong the overall network lifetime. Every node should store

information about the *security* (information about alerts and suspicious nodes) and the *environment* (list of the neighbors). In its *internal alert database*, the intrusion detection agent should store the security information generated by itself (containing time of creation, classification and source of the alert) [15].

Techniques

Pires et al. in [13] considered detection of *hello flood* and *wormhole* attacks in WSNs if a signal strength of a neighbor received by the IDS was incompatible with the assumed geographical positions of that neighbor. The detection was based on comparison of the received signal strengths with the expected values based on geographical information and the predefined transceiver specification. If some node was suspicious, the node that detected it broadcasted the information using *suspicious node information dissemination protocol*. However, the *localization* of the malicious nodes was left for the future work. Silva et al. in [14] defined rules that can be used for intrusion detection in WSNs. *Interval rule* can be used to measure the time between the reception of two consecutive packets. If it is too large, the intruder might not send data generated by a tampered node. If it is too small, the intruder may increment the packet sending rate in order to increase battery depletion of its neighbors. *Retransmission rule* can be used to find out whether packets supposed to be forwarded by a neighbor were forwarded or not to detect *selective forwarding* or *blackhole attack*. *Integrity rule* can be used to detect unauthorized modifications of the packets. *Delay rule* can be used to measure whether an intermediate node on the path delayed packets or not. *Repetition rule* can be used to measure whether a retransmission of the same packet exceeded predefined limit to detect *denial of service* or *jamming*. *Radio transmission range* can be used to measure whether all overheard packets were originated from one of the real neighbors to detect *wormhole* and *hello flood attack*. *Jamming rule* can be used to measure the number of collisions associated with a packet sent by the monitoring node to detect *jamming*. Roman et al. in [15] proposed that *local agents* should monitor attacks against logical and physical safety of the node (whether they are manipulated), measurements of the sensors (whether they follow certain patterns) and packets directly addressed to its node (whether they follow applied protocols). In addition, they should produce an alarm if a new neighbour is overheard or if a signal is *jammed*. *Global agents* should monitor primarily packet dropping and modification by analyzing communication of their neighbors. They can also behave as *spontaneous watchdogs*. If they hear a packet not addressed to them and the receiver is their neighbor, they monitor the forwarding of that packet with probability $1/n$, where n is the number of nodes that can monitor the same forwarding of the same packet as well.

III. CONCLUSION

The network operator considers the vulnerabilities and specifies the attacks exploitable by an attacker in order to compromise the network. In our work, we will focus on selective forwarding, delay and modification attacks, where the exchanged packets are monitored and thus storage overhead is generated. The detection techniques can be optimized to obtain sufficient accuracy at the cost of reasonable consumption of the resources. Another (if time and other resources permit) considered attack would be jamming, where parameters such as carrier sensing time[1] or number of retransmissions are monitored and corresponding threshold can be optimized. Last but not least, another potentially considered attack would be the Sybil attack, where the attacker's node changes its identity. The framework will be extendable to cover other techniques and to optimize them.

REFERENCES

[1]. Murat Dener, "Security Analysis in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2014

[2]. Kahina CHELLI," Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 1 - 3, 2015, London, U.K

[3]. Peng Zhou; Siwei Jiang; Irissappane, A.; Jie Zhang; Jianying Zhou; Teo, J.C.M., "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," in *Information Forensics and Security, IEEE Transactions on* , vol.10, no.3, pp.613-625, March 2015

[4]. Ching-Tsung Hsueh; Chih-Yu Wen; Yen-Chieh Ouyang, "A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks," in *Sensors Journal, IEEE* , vol.15, no.6, pp.3590-3602, June 2015

[5]. Martin Stehl´ık, Adam Saleh, Andriy Stetsko and Vashek Matya´s," Multi-Objective Optimization of Intrusion Detection Systems for Wireless Sensor Networks", Advances In Artificial Life, ECAL 2013

[6]. Raza, F.; Bashir, S.; Tauseef, K.; Shah, S.I., "Optimizing nodes proportion for intrusion detection in uniform and Gaussian distributed heterogeneous WSN," in *Applied Sciences and Technology (IBCAST), 2015 12th International Bhurban Conference on* , vol., no., pp.623-628, 13-17 Jan. 2015

[7]. Yun Wang; Weihuang Fu; Agrawal, D.P., "Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks," in *Parallel and Distributed Systems, IEEE Transactions on* , vol.24, no.2, pp.342-355, Feb. 2013

[8]. Nabil Ali Alrajeh, S. Khan, and Bilal Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 167575, 7 pages, 2013

[9]. Quazi Mamun, Rafiqul Islam, and Mohammed Kaosar," Anomaly Detection in Wireless Sensor

Network" Journal Of Networks, Vol. 9, No. 11, November 2014

[10]. D. E. Denning. An intrusion-detection model. *IEEE Transactions on Software Engineering*, (2):222–232, 1987

[11]. R. Heady, G. Lugar, M. Servilla, and A. Maccabe. The architecture of a network level intrusion detection system. Technical report, University of New Mexico, Albuquerque, NM, August 1990

[12]. Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 275–283, New York, NY, USA, 2000. ACM

[13]. W. R. Pires Jr, T. H. de Paula Figueiredo, H. C. Wong, and A. A. F. Loureiro. Malicious node detection in wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2004. 18th International Proceedings*, page 24, 2004.

[14]. A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. uiz, and H. C. Wong. Decentralized intrusion detection in wireless sensor networks. In *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pages 16–23, 2005.

[15]. R. Roman, J. Zhou, and J. Lopez. Applying intrusion detection systems to wireless sensor networks. In *IEEE Consumer Communications & Networking Conference (CCNC 2006)*, pages 640–644, Las Vegas (USA), January 2006

