IJRSET NOVEMBER 2017 Volume 4, Issue 11 Pages: 25-32

ISSN 2394-739X

IJRSET

International Journal for Research in Science Engineering and Technology

LITERATURE SURVEY ON SECURED WIRELESS SENSOR NETWORKS WITH DIFFERENT TYPES OF ATTACKS

[1] **P. E. Elango**
[1] **Ph.D Research Scholar,**
[1] **PG & Research Dept Of Computer Science,**
[1] **Periyar University, Salem, India.**

[2] **Dr. S. Subbaiah**
[2] **Assistant Professor,**
[2] **Department Of Computer Applications,**
[2] **Vivekananda College Of Arts & Science (Autonomous), India.**

ABSTRACT: Modern technological advancements in integrated circuit fabrication made it possible for the deployment of small, inexpensive, low-power, distributed devices to be capable of local processing and wireless communication. Such small devices are called sensor nodes, which are capable of only a limited amount of processing. The critical goal of WSNs security is to protect the wireless sensor networks from any types of attack. The different application scenarios presented in the earlier section point out those WSNs may have very different properties. Thus, considering the generic security requirements and application scenario the algorithm is developed to secure a WSN. The major properties that made the security mechanism challenging in WSNs are resource constraints, operational environment and unreliable communication. This survey paper provides survey on different mechanisms of attacks.

Keywords: - [Wireless sensor networks, attacks, internal attack]

1. INTRODUCTION

WSN’s technology has widely been used in our daily life. A typical WSN is shown in Figure 1 an event is detected in the sensor field and the information is routed to the sinker or base station then to the user with several communication media.

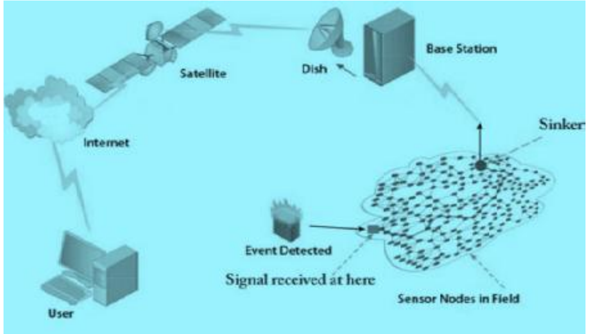

Figure 1- A Wireless Sensor Network

Wireless Sensor Networks have been applied to a range of applications, monitoring of space which includes environmental and habitat monitoring, indoor climate control, surveillance. Monitoring things example can be outlinedas structural monitoring, condition-based equipment maintenance. In addition, monitoring the interactions of things with each other and the surrounding space e.g., emergency response, disaster management, healthcare, energy sector. The majority of these applications may be split into two classifications: data collection and event detection.

The characteristics of WSNs lead a challenge to provide reasonable security to a network. The ultimate security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. In the case of internal attack the compromised node uses the legitimate network parameters to attack the network. In order to provide the reasonable security in WSNs all messages must maintain minimum security requirements. The standard requirements to provide security in a WSN are discussed as follows:

Confidentiality: An adversary can choose any node to eavesdrop as long as it iswithin the radio range due to the signals are transmitted over the opened channel. It is a threat for the data confidentiality as the attacker may gain the cryptographic information and take the information away.

Authentication: To determine the legitimate node and whether the received datahas come from the authorized sending node or not. Authentication is one of the key issues for a security.

Integrity: Information moving through the network could be altered or tamperedby others. Infect integrity is the description to trust the received information from the network.

Freshness: To save the network from the replay packets it is needed to ensurethat the received data is fresh and unused.

Secure management: It is necessary to manage the distribution of cryptographickeying material in the network.

2. LITERATURE REVIEW'S ON PRIOR WORKS

WSNs use multi-hop communication to increase network capacity. In multi-hop routing, messages may traverse many hops before reaching their destinations. However, simple sensor nodes are usually not well physically protected because they are cheap and are always deployed in open or hostile environments wherethey can be easily captured and compromised. An adversary can extract sensitive information, and control the compromised nodes. Even though let those nodes service for the attackers. Therefore, when a node is compromised, an adversary gains by accessing to the network and can produce malicious activities. The attacks are involved in corrupting network data or even disconnecting a major part of the network. To address the protection from internal attacks the following paragraphs discussed some existing mechanisms.

Zhang et al. in proposed a scheme that is the first and most cited work on intrusion detection in wireless ad hoc networks. Architecture is investigated for collaborative statistical anomaly detection which provides protection from attacks on ad hoc routing on wireless MAC protocols, or on wireless applications and services. Conceptually this architecture is divided into different modules. Firstly, Data collection; this module gathers streams of real time data form various sources. Secondly, using the local detection engine to analyze the local data traces gathered by the local data collections for evidence of anomaly and they suggested the statistical method for this stage. Detection methods need border data that requires collaboration among the nodes to be used in the cooperative detection. Intrusion responding actions are provided by both the local response and global response modules. Finally, secure communication module provides a high confidence communication channel to the agents. The advantage of this architecture is that they used statistical analysis. This architecture can only work on routing. For internal attack detection, it is not sufficient as it only focuses on routing protocol.

Silva et al. in proposed the first work on the rule based intrusion detection scheme to detect many different kinds of attacks in different layers. In this scheme three main phases are involved. Phase 1: data acquisition phase, in which the messages are filtered by the monitoring node to be analyzed. Phase 2: the rule application phase, which is responsible for applying the predefined rule to the stored data from the previous phase. Phase 3: the intrusion detectionphase, which compares the case between the numbers of raised failures produced from the rule application phase with a predefined number of occasional failures. If the total number of raised failures is higher than the predefined threshold, the alarm is raised.

According to Xieet al. this scheme presents a good framework to a class of rule-based intrusion detection. But, the main drawback of this scheme is the ambiguity in determining the number of monitoring nodes and the way of choosing them, such as how to make sure that the way of selection will cover the entire network. In addition, this scheme is restricted to some types of attacks, as the decision is made based on only a simple summation of the rule.

Karlof and Wagner discussed attacks at the network layer inand mentioned altered or replayed routing information and selective forwarding, node replication, Sybil attacks or black-grey-sink holes, and HELLO flooding. They suggested suitable countermeasures that can help to mitigate the attack. The solution discussed is prevention based and to secure the routing. This solution does not focus on the internal attacks or compromised node specifically.

Staddon et al proposed a way to trace the failed nodes in wireless sensor networks at the base station assuming that all the sensor measurement will be directed along the sinker based on a routing tree. The first step of the protocol enables the base station to learn the topology of the network. During the execution of many well-known route-discovery protocols, nodes learnt the identities of their neighbours. To convey this information to the base station, each node simply attaches a little bit of information about its neighbours to each of its measurements. In a constant amount of time the base station has adjacency information for the entire network and hence can construct its topology. Once the base station knows the node topology, the failed nodes can be efficiently traced using a simple divide-and-conquer strategy based on adaptive route update messages. In this work the sinker has the global view of the network topology and can identify the failed nodes through route update message.

Watchdog like techniques were discussed in the purpose of the watchdog mechanism is to identify a malicious node by overhearing the communication of the next hop. This technique can detect the packet dropping attack by letting nodes listen to the next hope nodes broadcasting transmission. From their research papers, each sensor node has its own watchdog that monitors and records its one hop neighbours'behaviours such as packet transmissions. When a sending node S sends a packet to its neighbour node T, the watchdog in S verifies whether T forwards the packet toward the Base Station (sink) or not by using the sensor's overhearing ability within its transceiver range. In this mechanism, S stores all recently sent packets in its buffer, and compares each packet with the overheard packet to see whether there is a match. If yes, it means that the packet is forwarded by T and S will remove the packet from the buffer. If a packet remains in the buffer for a period longer than a pre-determined time, the watchdog considers that T fails to forward the packet and will increase its failure tally for T. If a neighbour's failure tally exceeds a certain threshold, it will be considered as a misbehaving node by S. But, multiple watchdogs need to work collaboratively in decision making. A reputation system is necessary to provide the quality rating of the participants. This method will fail when the following matters happened, ambiguous collision,receiver collision, limited transmission power, false misbehaviour, and partial dropping.

A machine learning based approach is proposed by Huang and Lee in for anomaly detection. They developed a cross feature analysis anomaly detection approach that explores the co-relation between each feature and all other features for the nodes. This is conducted by computing classifiers from a training set composed of normal nodes. An intrusion alarm is raised if the correlation between the features does not match those of the classifiers. The machine learning procedure assumes a large number of features being monitored from sensor behaviours, and the availability of normal sensors as the training data set, both of which are difficult to obtain considering the restrained sensor resources and dynamic networking behaviours.

Pireset al. in presented a solution to identify malicious nodes in wireless sensor networks through detection of malicious message transmissions in a network based on the signal strength. A message transmission is considered suspicious if its signal strength is incompatible with its originator's geographical position. The geographical position is determined by the Global Positioning System (GPS). In this work they showed how to detect HELLO flood attack and the wormhole attack by comparing the energy of the received signal and the energy of the same observed signal around the network. This is work use GPS for location detection. Thus, this system can only be implemented in the line of sight scenario and restricted with HELLO flood attack and the wormhole attack. In addition, the signal strength can be infected by other factors such as interference from electronic devices, environmental factors for example, rain and storm.

Branch et al. in studied the in network outlier. They developed an algorithm that has the following properties: (i) it is generic – suitable for many outliers detection heuristics; (ii) it works in networks with a communication load proportional to the outcome that is the number of outliers reported; (iii) it is robust with respect to data and network change; (iv) the outcome is revealed to all of the sensors. In other words, in this method each sensor in the network first identifies the outliers based on the neighbourhood data. Then exchange the decision with neighbours to achieve the global set of outliers. But this method does not work well for small system with limited samples. In addition, it is expensive as well as it depends on the neighbour collaboration.

Support Vector Machine (SVM), based on techniques for internal attack detection in sensor data was proposed in this technique uses one-class quarter-sphere SVM to reduce the effort of computational complexity and locally identify outliers at each node. The sensor data that lies outside the quarter sphere is considered as an outlier or internal attack. Each node communicates only summary information (the radius information of sphere) with its parent for global outlier classification. This technique identifies outliers from the data measurementscollected after a long time accumulation within a window. The technique also ignores spatial correlation of neighbour nodes, which makes the results of local outliers inaccurate. The main drawback of SVM-based techniques is their computational complexity and hard for the choice of proper kernel function.

Zhang et al. in proposed a distance-based technique to identify n global outliers in snapshot and continuous query processing applications of sensor networks. This technique reduces communication overhead as it adopts the structure of aggregation tree and prevents broadcasting of each node in the network. Each node in the tree transmits some useful data to its parent after collecting all the data sent from its children. The sink node then roughly figures out top n global outliers and floods these outliers to all the nodes in the network for verification. If any node disagrees on the global results, it will send extra data to the sink node again for outlier detection. This procedure is repeated until all the nodes in the network agree on the global results calculated by the sink node. This technique considers only one-dimensional data and the aggregation tree used may not be stable due to the dynamic changes of network topology.

Recently Game theory is commonly used to analyze wireless sensor networks with selfish/attacker nodes. Reddy and Ma studied game theory, Reddy et al. presented in zero-sum game which may find malicious sensor nodes in the forwarding path only. Zero-sum game method needs to maintain a certain level of energy. The proposed game theory method in not only improves the security of WSNs, but also reduces the cost caused by monitoring sensor nodes and prolongs the lifecycle of each sensor node. However, the method does not consider the effects of the compromised entity of the sensor nodes, which can discard normal packets or not transfer normal packets in WSNs.

The fuzzy logic based intrusion detection approach has been widely used and studied such as by Chi and Moon. In node energy, transmission rate, lists of the neighbour nodes and transmission errors are taken as themeasurement parameter. Based on the four features the base station will take the decision about the denial of service (DoS) attacks. In the approach is to detect sinkhole attacks in directed diffusion based sensor networks based on the radio and transmission radius. In a sinkhole attack, there will be extra message traffic in area compare to the normal traffic and the transmission radius will be smaller. The fuzzy logic system will produce detection value based on the normal traffic and transmission radius. The decision will be taken based on the predefined threshold and the fuzzy rules need to be set according to the symptoms with extensive study of sinkhole attack. The main drawback of the fuzzy logic is that it needs the manual settings of rules in this method.

Stetskoet al. implemented an intrusion detection system which employs the neighbour based detection technique. They designed the system to work on the TinyOS operating system running the Collection Tree Protocol. They used selective forwarding, jamming and hello flood attacks to evaluate the system. In their work, the nodes collaboration among themselves is efficient as at the same time it generates the communication overhead. This method suffers from false alarm for packet dropping and sending rate. Moreover, this method does not consider the power consumption rate related to the network performance.

A collaborative and decentralized approach for an intrusion detection system was proposed by Lemoset al. to detect node repetition attacks. In this scheme some special nodes, called monitors, will be responsible for monitoring the behaviour of neighbour nodes in turn by using predefined rules. The malicious activities evidence discovered by each monitor will be shared and correlated with the purpose of increasing the accuracy in detection of intruders. This paper also claimed that it was a robust method with two layers of protection. The drawback of this method is the monitor nodes could be compromised, which were not to be considered. It is a rule based approach that has an assumption of the parameters that need to be made. Therefore, it has inflexibility for applications.

An integrated approach is proposed by Wang et al. this method can provide the system to resist intrusions, and process in real-time by analysing the attacks. The Integrated Intrusion Detection System (IIDS) includes three individual Intrusion Detection Systems (IDSs): (i) Intelligent Hybrid IntrusionDetection System (IHIDS); (ii) Hybrid Intrusion Detection System (HIDS); and Misuse Intrusion Detection System (MIDS). The goal is to raise the detectionrate and lower the false positive rate through misuse detection and anomaly detection. Finally, a decision-making module is used to integrate the detected results and report the types of attacks. The advantage of this method is that it is suitable for design of detection modules based on capabilities and probabilities of getting compromised. The use of back propagation method in building the detection module implies high computational complexity. In addition it has low detection accuracy and high false alarm.

Bankovicet al. proposed a machine learning solution for anomaly detection. This combines with the feature extraction process that tries to detect temporal and spatial inconsistencies. It uses the sequences of sensed values buy nodes and the routing paths used to forward these values to the base station. The data produced in the presence of an attacker are treated as outliers and detected using clustering techniques. The techniques are coupled with a reputation system to isolate the compromised node. A drawback of this system is that the system cannot use all the information of the nodes since the nodes cannot share their bad experiences such as dropped packets. This is particularly detrimental since learning from one's own experience in this scenario comes at a very high price.

A dual-weighted trust evaluation in a hierarchical sensor network is proposed by Hyun et al. [108]. In this method sensor nodes report their readings to a forwarding node for aggregation. Each sensor node need to assigned two trust values. They are increased or decreased depending on its reading and the aggregation results at the forwarding node. An updating policy is developed tokeep misdetection rates low while achieving high malicious node detection rate for a wide range of fault and related probabilities. But, the performance of a malicious node detection scheme depends on the correctness of the aggregation and results at the forwarding node, since wrong decisions at the node lead to inaccurate management of trust values. The resulting false alarms might waste energy and thus shorten the network lifetime.

Znaidiet al. addressed the problem of nodes replication attacks. They first introduced a hierarchical distributed algorithm for detecting node replication attacks using a Bloom filter mechanism and a cluster head selection. The algorithm works as soon as the network is built upon a cluster head selection mechanism generating a three-tier hierarchy. In this method, each cluster head exchanges the member nodes identifications (IDs) through a Bloom filter with the other cluster heads to detect eventual node replications. However, this method needs to employ additional clustering algorithm and the authors presented only a theoretical discussion on the boundaries.

Garofaloet al. in proposed a new intrusion detection system architecture designed to ensure a trade-off between different requirements. It is high detection rate obtained through decision tree classification. By which the energy saving is obtained through light detection techniques on the motes. But, in this method the power consumption is high, it is not resilient to node failures as it uses a tree classification, with a long delay to send the data to the base station, data overhead is high and it is costly.

A few papers also addressed pollution attacks in internal flow coding systems employing special crafted digital signaturesor hash functions. Recently some papers discussed preventing the internal attacks by related protocols but looking at protocol does not protect the WSN completely.

3. DIFFERENT THREATS AND DIFFERENT ATTACKS

THREAT	INTERNAL\EXTERNAL	THREAT CONSEQUENCES
e-mail with virus	External origination, internal use	Could infect system reading email and subsequently spread throughout entire organizing
Network virus	External	Could enter through unprotected ports, compromise
Web based virus	Internal browsing to external site	Could cause compromise on system doing browsing and subsequently affect other internal to network
Web server attack	External to web servers	If web server is compromise hacker could gain access to other systems internal to network

Denial of service attack	External	External Services such as web,email and ftp could become unusable If router is attacked, whole network could go down
Network User Attack (internal Employee)	Internal to anywhere	Traditional border firewalls do nothing for this attack internal segmentation firewalls can help contain damage.

CONCLUSION

In this survey paper, special care will be taken with the challenges for the current wireless sensor network. This paper discussed the WSNs evaluation, characteristics, architecture, protocols, applications, security and suggested mechanisms, which lead us to investigate what the gaps between the current and future challenges which lead this research direction.

REFERENCES

[1]. L. K. Bysani and A. K. Turuk, "A Survey on Selective Forwarding Attackin Wireless Sensor Networks," in 2011 International Conference on Devicesand Communications (ICDeCom), Feb., pp. 1–5.

[2]. T. H. Hai and E.-N. Huh, "Detecting Selective Forwarding Attacks inWireless Sensor Networks Using Two-hops Neighbor Knowledge," in SeventhIEEE International Symposium on Network Computing and Applications,2008. NCA '08, 2008, pp. 325–331.

[3]. Y. Chen, W. Trappe, and R. P. Martin, "Detecting and Localizing WirelessSpoofing Attacks," in 4th Annual IEEE Communications Society Conferenceon Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07, June, pp. 193–202.

[4]. Y. Zhang and W. Lee, "Intrusion Detection in Wireless AdHoc Networks,"presented at the ACM MOBICOM, The Annual International Conference onMobile Computing and Networking, Boston, Massachusesttes, USA, 2000, pp.275–283.

[5]. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B.Ruiz, and H. C. Wong, "Decentralized Intrusion Detection in Wireless SensorNetworks," in Proceedings Of The 1st ACM International Workshop OnQuality Of Service & Security in Wireless And Mobile Networks(Q2SWINET'05), 2005, pp. 16–23.

[6]. M. Xie, S. Han, B. Tian, and S. Pravin, "Anomaly detection in wirelesssensor networks: A survey," Journal of Network and Computer Applications,vol. 34, no. 4, pp. 1302–1325, Jul. 2011.

[7]. J. Staddon, D. Balfanz, and G. Durfee, "Efficient tracing of failed nodes insensor networks," in Proceedings of the 1st ACM international workshop onWireless sensor networks and applications, New York, NY, USA, 2002, pp.122–130.135

[8]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routingmisbehavior in mobile ad hoc networks," in Proceedings of the 6th annualinternational conference on Mobile computing and networking, New York,NY, USA, 2000, pp. 255–265.

[9]. K. Paul and D. Westhoff, "Context aware detection of selfish nodes in DSRbased ad-hoc networks," in IEEE Global Telecommunications Conference,2002. GLOBECOM '02, 2002, vol. 1, pp. 178 – 182 vol.1.

[10]. S. Bansal and M. Baker, "Observation-based Cooperation Enforcement inAd hoc Networks," Research Report, cs.NI/0307012, vol. 2, no. 1, pp. 1–10,Jul. 2003.

[11]. Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hocnetworks," in Proceedings of the 1st ACM workshop on Security of ad hoc andsensor networks, New York, NY, USA, 2003, pp. 135–147.

[12]. J. Pires, W.R., T. H. de Paula Figueiredo, H. C. Wong, and A. A. F.Loureiro, “Malicious node detection in wireless sensor networks,” in Paralleland Distributed Processing Symposium, 2004. Proceedings. 18th International, 2004, p. 24.

[13]. J. Branch, B. Szymanski, C. Giannella, R. Wolff, and H. Kargupta, “In-Network Outlier Detection in Wireless Sensor Networks,” in 26th IEEEInternational Conference on Distributed Computing Systems, 2006. ICDCS2006, 2006, p. 51.

[14]. S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, “QuarterSphere Based Distributed Anomaly Detection in Wireless Sensor Networks,”in IEEE International Conference on Communications, 2007. ICC ’07, 2007,pp. 3864 –3869.

[15]. K. Zhang, S. Shi, H. Gao, and J. Li, “Unsupervised Outlier Detection inSensor Networks Using Aggregation Tree,” in Proceedings of the 3rdinternational conference on Advanced Data Mining and Applications, Berlin,Heidelberg, 2007, pp. 158–169.136

[16]. Y. B. Reddy, “A Game Theory Approach to Detect Malicious Nodes inWireless Sensor Networks,” in Third International Conference on SensorTechnologies and Applications, 2009. SENSORCOMM ’09, June, pp. 462–468.

[17]. Y. Ma, H. Cao, and J. Ma, “The intrusion detection method based on gametheory in wireless sensor network,” in 2008 First IEEE InternationalConference on Ubi-Media Computing, 2008, pp. 326–331.

[18]. S. H. Chi and T. H. Cho, “Fuzzy logic anomaly detection scheme fordirected diffusion based sensor networks,” in Proceedings of the Thirdinternational conference on Fuzzy Systems and Knowledge Discovery, Berlin,Heidelberg, 2006, pp. 725–734.

[19]. S. Y. Moon and T. H. Cho, “Intrusion Detection Scheme Against SinkholeAttacks in Directed Diffusion Based Sensor Networks| Whitepapers |TechRepublic,” Intrusion detection scheme against sinkhole attacks indirected diffusion based sensor networks, vol. 9, no. 7, pp. 118–122, Jul. 2009.

[20]. M. V. de S. Lemos, L. B. Leal, and R. H. Filho, “A New CollaborativeApproach for Intrusion Detection System on Wireless Sensor Networks,” inNovel Algorithms and Techniques in Telecommunications and Networking, T.Sobh, K. Elleithy, and A. Mahmood, Eds. Springer Netherlands, 2010, pp.239–244.

[21]. S.-S. Wang, K.-Q. Yan, S.-C. Wang, and C.-W. Liu, “An IntegratedIntrusion Detection System for Cluster-based Wireless Sensor Networks,”Expert Systems with Applications, vol. 38, no. 12, pp. 15234–15243, Nov.2011.

[22]. Z. Banković, J. M. Moya, J. C. Vallejo, and D. Fraga, “Detecting UnknownAttacks in Wireless Sensor Networks Using Clustering Techniques,” inHybrid Artificial Intelligent Systems, E. Corchado, M. Kurzyński, and M.Woźniak, Eds. Springer Berlin Heidelberg, 2011, pp. 214–221.