Wireless Sensor Networks: A Survey Analysis of Safety and Proficient Attacker's Issues

M.Mahadevan, Research Scholar, Karpagam University, Coimbatore, TamilNadu.
Dr. G. Tholkappia Arasu, Principal, AVS Engineering College, Salem, TamilNadu.

Abstract:

The wireless sensor network is a booming network widely used by all the sectors for the communication purpose in an efficient way. In that the issues of the network such as security, efficiency in cost, energy and reliability in the communication are the major research areas. The survey of the paper is mainly concentrate on the security issues. Because focusing the security issues it will automatically step down the misbehavior nodes which leads to reliable communication and it increase the efficiency of the networks. The attacks in WSNs are increased as day by day in this contemplate concentrate on injecting false data, Node Compromise, False Node, Sinkhole Attacks, Hello Flood Attacks and so on. And also in this survey it discussed the techniques and schemes to overcome these attacks.

Keywords: Wireless Sensor Network, security issues, misbehaving nodes, injecting false data, identifying the attacks.

Introduction

A **wireless sensor network (WSN)** of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of nodes from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

Types of attacks in WSN

In WSNs lot of attacks are available such as Selective forwarding, Wormholes, Sybil attacks, injecting false data attack, Passive Information Gathering and Message Corruption, Node Compromise, Node Tampering, False Node, Node Outage, Traffic

Analysis, Acknowledgement Spoofing, Spoofed, Altered or Replayed Routing Information, Sinkhole Attacks, Hello Flood Attacks, DoS (Denial of Service) Attacks.

Literature review

The research of Intrusion Detection Systems (IDS) is a mature area in wired networks, and has also attracted many attentions in wireless ad hoc networks recently. The general guidelines for applying IDS to static sensor networks, and introduce a novel technique to optimally watch over the communications of the sensors neighborhood on certain scenarios were discussed. The main goal of the solution is to activate only one global agent per packet circulating in the network. IDS solutions created for ad hoc wireless networks cannot be applied directly to sensor networks, and introduce the general guidelines for applying IDS architectures in static sensor networks (with no mobile nodes). Also, a novel technique for optimally monitoring neighbors, that have called spontaneous watchdogs, was introduced. A general IDS architecture for static sensor networks, and introduced a new technique, the spontaneous watchdogs, where some nodes are able to choose independently to monitor the communications in their neighborhood was proposed. The implementation and simulation of the architecture over a particular group of protocols in order to study the energy consumption and IDS performance of this model were discussed. There are other factors that must be thoroughly investigated, such as how a node can deduce the number of neighbors that can activate their global agents if no additional information is available (e.g. when nodes cannot store the complete neighbors list), how real-life radio models can affect the spontaneous watchdog technique, how to successfully aggregate alert data in a flat network, and other issues [5].

Two techniques that improve throughput in an adhoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem a categorizing nodes based upon their dynamically measured behavior was proposed. Watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. Through simulation watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. Ad hoc networks are an increasingly promising area of research with practical applications, but they are vulnerable in many settings to nodes that misbehave when routing packets. For robust performance in an untrusted environment, it is necessary to resist such routing misbehavior but they are vulnerable in many settings to nodes that misbehave when routing packets. For robust performance in an untrusted environment, it is necessary to resist such routing misbehavior. Two possible extensions to DSR to mitigate the effects of routing misbehavior in ad hoc networks the watchdog and the pathrater were analyzed [4].

Sensor networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects false data into the network with the goal of deceiving the base station or depleting the resources of the relaying nodes. Standard authentication mechanisms cannot prevent this attack if the adversary has compromised one or a small number of sensor nodes. An interleaved hop-by-hop authentication scheme that guarantees that the base station will detect any injected false data packets when no more than a certain number t nodes are

compromised was presented. Further, the scheme provides an upper bound B for the number of hops that a false data packet could be forwarded before it is detected and dropped, given that there are up to t colluding compromised nodes. That in the worst case B is O (t2). Through performance analysis, it shows that the scheme is efficient with respect to the security it provides, and it also allows a tradeoff between security and performance.

Unattended sensor node deployment also makes another attack easier: an adversary may compromise several sensor nodes, and then use the compromised nodes to inject false data into the network. This attack falls in the category of insider attacks. Standard authentication mechanisms are not sufficient to prevent such insider attacks, since the adversary knows all the keying material possessed by the compromised nodes. This attack can be launched against many sensor network applications, though military scenario was taken for an example. A scheme for addressing this form of attack, which called as a false data injection attack, was presented. This scheme enables the base station to verify the authenticity of a report that it has received as long as the number of compromised sensor nodes does not exceed a certain threshold. Further, the scheme attempts to filter out false data packets injected into the network by compromised nodes before they reach the base station, thus saving the energy for relaying them. Simple but effective authentication scheme to prevent false data injection attacks in sensor networks was presented. This scheme guarantees that the base station can detect a false report when no more than t nodes are compromised, where t is a security threshold. In addition, the scheme guarantees that t colluding compromised sensors can deceive at most B non compromised nodes to forward false data they inject, where B is O (t2) in the worst case. The performance analysis shows this scheme is efficient with respect to the security it provides and allows a tradeoff between security and performance. Moreover the scheme presented in this it describe, that a false data packet injected into the network will be detected within one hop, i.e., B = 0. This improvement is achieved at the expense of additional computational overhead per node, although the communication overhead of both schemes is identical [8].

A compromised node can inject into the network large quantities of bogus sensing reports which, if undetected, would be forwarded to the data collection point (i.e. the sink). Such attacks by compromised sensors can cause not only false alarms but also the depletion of the finite amount of energy in a battery powered network. A Statistical En-route Filtering (SEF) mechanism that can detect and drop such false reports was presented. SEF requires that each sensing report be validated by multiple keyed message authentication codes (MACs), each generated by a node that detects the same event. As the report is forwarded, each node along the way verifies the correctness of the MACs probabilistically and drops those with invalid MACs at earliest points. The sink further filters out remaining false reports that escape the en-route filtering. SEF exploits the network scale to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding nodes.

Sensor networks serving mission-critical applications are potential targets for malicious attacks. Although a number of recent research efforts have addressed security issues such as node authentication, data secrecy and integrity, they provide no protection

against injected false sensing reports once any single node is compromised. SEF aims at detecting and dropping such false reports injected by compromised nodes. It takes advantage of the large scale and dense deployment of sensor networks. The analysis and simulation results show that SEF can effectively detect false reports even when the attacker has obtained the security keys from a number of compromised nodes, as long as those keys belong to a small number of the key pool partitions. SEF represents a first step towards building resilient sensor networks that can withstand compromised nodes. SEF achieves this goal by carefully limiting the amount of security information assigned to each individual node. On the other hand, collaborative filtering of false reports requires that nodes share certain amount of security information. The more security information each forwarding node possesses, the more effective the en-route filtering can be, but also the more secret the attacker can obtain from a compromised node. The plan for the next step includes evaluation of the tradeoffs between these two conflict goals, and gaining further insight on how to build a sensor network that can be at once resilient against many compromised nodes as well as effective in detecting false data reports through collaborative filtering [7].

Global synchronization is crucial to many sensor network applications that require precise mapping of the collected sensor data with the time of the events, for example in tracking and surveillance. It also plays an important role in energy conservation in MAC layer protocols. Three methods to achieve global synchronization in a sensor network: a node-based approach, a hierarchical cluster based method, and a fully localized diffusion-based method were discussed. The synchronous and asynchronous implementations of the diffusion-based protocols were given. The global synchronization problem in sensor networks is a major issue. The all-node-based method, the cluster based method, and the diffusion-based methods to solve the problem. The first two methods require a node to initiate the global synchronization, which is neither fault-tolerant nor localized. In the diffusion-based method, each node can perform its operation locally, but still achieve the global clock value over the whole network. It presents two implementations of the clock diffusion: synchronous and asynchronous. The synchronous method assumes all the nodes perform their local operations in a set order, while the asynchronous method relaxes the constraint by allowing each node to perform its operation at random. It presents the theoretical analysis of these methods and show simulation results for the asynchronous averaging synchronization method. The algorithms can be extended to other sensor network applications, such as data aggregation was presented [12].

Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. A security goal for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols. Crippling attacks against all of them and suggests countermeasures and design considerations were discussed. This is the first such analysis of secure routing in sensor networks. Secure routing is vital to the acceptance and use of sensor networks for many applications, but it have demonstrated that currently proposed routing protocols for these

networks are insecure. Leave it as an open problem to design a sensor network routing protocol that satisfies proposed security goals. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote-class outsiders, but cryptography alone is not enough. The possible presence of laptop-class adversaries and insiders and the limited applicability of end to- end security mechanisms necessitates careful protocol design as well [2].

A resilient packet-forwarding scheme using Neighbor Watch System (NWS), specifically designed for hop-by-hop reliable delivery in face of malicious nodes that drop relaying packets, as well as faulty nodes that fail to relay packets were introduced. Unlike previous work with multipath data forwarding, this scheme basically employs single-path data forwarding, which consumes less power than multipath schemes. As the packet is forwarded along the single-path toward the base station, this scheme, however, converts into multipath data forwarding at the location where NWS detects relaying nodes' misbehavior. Experiments show that, with the help of NWS, the forwarding scheme achieves a high success ratio in face of a large number of packet-dropping nodes, and effectively adjusts its forwarding style, depending on the number of packet-dropping nodes en-route to the base station. In face of such nodes, NWS is specifically designed for hop-by-hop reliable delivery, and the prompt reaction of the conversion from single-path to multipath forwarding augments the robustness in the scheme so that the packet successfully reaches the base station. Further improving NLV to defend against the man-in-the-middle attacks, collusion among compromised nodes were discussed. Such attacks can be prevented by using a master key derived with not only a node ID but also its geographic information [6].

Node compromise poses severe security threats in wireless sensor networks. Unfortunately, existing security designs can address only a small, fixed threshold number of compromised nodes; the security protection completely breaks down when the threshold is exceeded. To overcome the threshold limitation and achieve resiliency against an increasing number of compromised nodes were seeked. A novel location-based approach in which the secret keys are bound to geographic locations, and each node stores a few keys based on its own location. The location-binding property constrains the scope for which individual keys can be (mis)used, thus limiting the damages caused by a collection of compromised nodes. These approaches through the problem of report fabrication attacks, in which the compromised nodes forge non-existent event, are illustrated. The design through extensive analysis, implementation and simulations, and demonstrate its graceful performance degradation in the presence of an increasing number of compromised nodes were evaluated. Node compromise presents severe security threats in sensor networks. Existing solutions either do not address such insider attacks, or completely break down when more than a fixed threshold number of nodes are compromised.

LBRS aims at providing resilient security and graceful performance degradation against an increasing number of compromised nodes. It achieves resiliency by limiting the scope for which keys are used. Different from the existing work that binds keys to nodes, LBRS binds keys to geographical locations. This ensures that the keys can only be used to endorse local events where they are bound. The attacker can no longer abuse the compromised keys

for global usage, such as fabricating events in arbitrary locations. As one general design guideline, constraining the scope for which secrets are used can lead to higher degree of resiliency. However, in symmetric-key based designs, the same secret key is used for two different functions: credential generation and verification. Had these two functions relied on different secrets (e.g., as in public-key cryptography), compromise of verifying nodes leads to little harm because the verification secret cannot be used to forge credentials. The location binding keys offer an alternative way to limit the scope of key usage. That such a location-based design approach can achieve resilient security in an efficient and scalable fashion. It provides a balance between secret sharing and secret separation. It enables the sensor nodes to collaborate in securing the network by sharing symmetric keys, yet limits the scope and usage of individual keys [9].

WSN nodes face many challenges starting from deployment till their life span which is dependent on very low battery strength. Since these nodes are operated in unattended environments, many security threats are for them to survive. These nodes face variety of attacks at different layers of their architecture, ranging from physical stealing, tempering to reprogramming. Applying any traditional security mechanism over wireless sensor nodes is also not possible as those traditional algorithms or protocols consume very much processing and power due to their complexity. In this paper the WSN primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self-Organization, Time Synchronization and Secure Localization.

The attacks of WSN can be classified into two categories: invasive and non-invasive. Non-invasive attacks generally target to timings, power and frequency of channel. Invasive attacks target to availability of service, transit of information, routing etc. In DoS attack, hacker tries to make service or system inaccessible.

- **Attacks at Physical Layer**

  Jamming, Tempering

- **Attacks at Link Layer**

  Exhaustion (Continuous Channel Access), Collision, Unfairness

- **Attack s at Network Layer**

  False Routing or Spoofed, Altered, Replayed Routing Information, Selective Forwarding, Sinkhole Attacks, Sybil Attack, Wormhole, Hello Flood.

Any traditional security mechanism can also not be applied at any level of WSN architecture to prevent for its respective attacks as nodes will not be able to execute same mechanism or will be exhausting their power and life. Large scale deployment for tightening the security measures are also not possible over low capability nodes [10].

WSNs are often deployed in harsh environments, where an attacker node can physically capture some of the sensor nodes. Once a sensor node is captured then the attacker node can collect all the credentials like keys, identities etc. The attacker can modify the message and replicate in order to overhear the messages or interrupt the functionality of the sensor networks. IPD and PSD are proposed as an optimized localization algorithm for defending against the node

replication attacks. Herein, two replica detection algorithms for wireless sensor networks (WSNs) IPD and PSD are proposed. Although IPD is not resilient against collusive replicas, its detection framework, *challenge-and-response*, is considered novel as compared with the existing algorithms. IPD protocol is based on remember *and challenge* strategy for detecting node replication attacks in mobile networks.

A unique feature of IPD is that each node is capable of detecting replicas per move, which contrasts sharply with other protocols that need to mobilize the whole network for replica detection. PSD not only achieves balance among storage, computation, and communication overheads, which are all, but also possess unique characteristics, including network-wide time synchronization avoidance and network-wide revocation avoidance, in the detection of node replication attacks [13].

Wireless Sensor Network (WSN) is an emerging technology with the purpose of demonstrating immense promise for various innovative applications such as traffic surveillance, building, smart homes, habitat monitoring and many more scenarios. The sensing technology joint with dispensation control and wireless communication makes it beneficial for being exploited excess in future. The addition of wireless communication technology as well acquires a variety of security threats. The intention of this paper is to examine the security related problems and challenges in wireless sensor networks. This paper discusses a broad diversity of attacks in wireless sensor network and their classification mechanisms and different security schemes available to handle them as well as the challenges faced.

Generally most of the attacks beside security in wireless sensor networks are caused by insertion of fake data or information through the compromise nodes inside the network. For shielding the inclusion of fake information by compromise nodes, a means is necessary for sensing fake information. On the other hand, developing such a detection mechanism and creating it proficient signifies an immense research challenge. This paper described the attacks and their classifications in wireless sensor networks as well as makes an effort to discover the security mechanism extensively use to handle these attacks [14].

Mobile ad hoc networks are susceptible to safety attacks from hateful nodes due to their wireless and dynamic nature and essential safety component in it is certificate revocation. Protecting genuine nodes from hateful attacks must be considered in mobile ad hoc networks which are attainable all the way through employment of key management system which serves as a means of assigning conviction in public key communications. The most accepted method is a trouble-free certificate control approach by using a certificate revocation list which is managed by a single or shared multiple certificate authority. The certificate of a suspicious node is retracted when summation of weights of votes in opposition to node go beyond a predefined threshold. A voting-based scheme is proposed so that it allows all nodes in the network to vote. There is still a remaining issue in coping with collusion attacks by multiple malicious attackers although ubiquitous and robust access control for mobile ad hoc networks is robust for false accusation attacks. As with ubiquitous and robust access control for mobile ad hoc networks, no certificate authority exists in the network. Threshold based mechanism was introduced to restore the accusation function of nodes in the warning list in order to address the issue of the

number of normal nodes being gradually reduced [15].

Conclusion:

This survey discussed about the security issues in the Wireless Sensor Networks and the types of security attacks. More number of techniques are used to identify the security attacks and the schemes are introduced to overcome those attacks. In that techniques the misbehaving nodes are identified with the help of watch dog, injecting false data and sinkholes are the single path method identification. Some difficulties arises due to single path method to overcome this the multipath methods are introduced and handled successfully.

References:

[1] H.Chan and A. Perrig, "Security and Privacy in Sensor Networks," *IEEE Computer*, October 2013.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, May 2013.

[3] V. Bhuse, A. Gupta, and L. Lilien, "Dpdsn: Detection of packet-dropping attacks for wireless sensor networks," *In the Trusted Internet Workshop, International Conference on High Performance Computing*, December 2012.

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *ACM MobiCom*, August 2013.

[5] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," *Third IEEE Annual Consumer Communications and Networking Conference (CCNC)*, pp. 640–644, Jan. 2012.

[6] S. Lee and Y. Choi, "A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks," *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks (SASN)*, pp. 59–70, 2013.

[7] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-route Filtering of Injected False Data in Sensor Networks," *IEEE INFOCOM*, March 2014.

[8] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data in Sensor Networks," *IEEE Symposium on Security and Privacy*, 2014.

[9] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, May 2013.

[10] Z. Yu and Y. Guan, "A Dynamic En-route Scheme for Filtering False Data in Wireless Sensor Networks," *IEEE Infocom 2006*, April 2013.

[11] F. Ye, H. Yang, and Z. Liu, "Catching Moles in Sensor Networks," *IEEE International Conference on Distributed Computing Systems (ICDCS)*, June 2014.

[12] Q. Li and D. Rus, "Global clock synchronization in sensor networks," *IEEE INFOCOM*, 2013.

[13] Sunil Ghildiyal, Ashish Gupta, "ANALYSIS OF WIRELESS SENSOR NETWORKS: SECURITY, ATTACKS AND CHALLENGES", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308, 2014.

[14] R.M.Sinthiya, J.Vijipriya,"An Optimized Localization Algorithm against Node Replication Attacks in Wireless Sensor Networks", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 2 Page No.3817-3821, February 2014.

[15] Gursewak Singh, Rajni Bedi, "A Survey of Various Attacks and Their Security Mechanisms in Wireless Sensor Network", International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-2, Issue-8, June 2014.