ISSN:2231-0711
www.ijcset.net

Methods of Protecting Data in a Wireless Network

Amir Massoud Bidgoil [#1], Maryam Amanifar[*2], Ali Pajoohanfar [†3]

[#]*Department of computer engineering, Islamic Azad University, Tehran North Branch, Tehran, Iran*
am_bidgoli@iau-tnb.ac.ir

[*]*Khoramshahr Branch, Islamic Azad University, Khoramshahr, Iran*
m.amanifar@khouzestan.srbiau.ac.ir

[†]*SAMA Technical and Vocational Training College, Islamic Azad University, Ahvaz, Iran*
a.pajooh@gmail.com

Abstract— **Wireless Sensor Networks (WSNs) consist of hundreds of sensor nodes often deployed in an unsecured or in hostile environment. Wireless sensor networks have been deployed in insecure environments. The wireless sensor networks used in military applications, health, industrial used In this paper we describe methods for dealing with security goals.**

Keywords— **Sensor Networks,Wireless,Data ,Data security.**

I.INTRODUCTION

Wireless Sensor Networks consists number of autonomous distributed sensors nodes to monitor physical or environmental conditions such as sound, pressure, temperature, vibration etc., the development of Wireless Sensor Networks was first initiated by military applications such as battlefield surveillance and now these are emerged into various fields such as industrial process monitoring, health monitoring and traffic control etc [1, 3, 4, 6]. WSNs are built of nodes from few to several hundreds and thousands of sensors nodes which are connected through wireless media. The data is travelled from event of interest to destination through multiple hops. In some applications where data plays an important role, the data should be secured so that only intended receiver should receive the data.

One of most threat in WSNs is compromise of sensor nodes [9]. The attackers can compromise single node to multiple nodes to acquire such keying information. Due to the increase of compromised nodes in Sensor Networks this leads to security threats. The WSNs must be deployed in such an environment such that authenticity, confidentiality and availability should be achieved. Along with these the attackers make use of the compromised nodes to introduce the false information or data into environment which leads to more traffic into network and thus slow down the communication overhead between nodes and leads to more energy consumption. In this paper we are going to define what attacks are, how the wireless environment should be, how to achieve authenticity, confidentiality, availability and how to organize the data in order to achieve good performance and to minimize the energy consumption in order better use of resources in Wireless Sensor Networks.

II. DESIGN OF WSN ENVIRONMENT

Wireless sensor network environment are often deployed in an environment where the nodes communicate through wireless media, as a result these are subjected to insider and outsider attacks.

Many researches were made for the deployment of nodes in wireless sensor networks [7]. Most of them define the environment in grid fashion so that the targeted terrain consists of number of cells with this the maintenance and control of the cells can be easily done rather than considering the whole environment as a single unit. In WSNs the nodes are scattered in different locations and there should me mechanisms to find out the position of nodes and where the nodes are attacked and dead nodes should be identified. Insider attacks can give incorrect position and distance information in order to give false information about their position. External attackers can manipulate the measured positions and distances between wireless sensor nodes. The deployment of nodes in WSNs is dependent on the application and can be either randomized or manual [7, 6]. In manual deployment sensors nodes are positioned manually and data is transmitted through paths which are defined prior. In random deployment of sensor nodes the nodes are distributed randomly. If the distribution is not uniform optimal clustering of nodes becomes necessary to allow the connectivity and enabling efficient energy network operation. Researchers have proposed many positioning and distance estimation techniques however all these have adversarial setting. Global Positioning systems (GPS) [7, 6] are not suitable for indoor positioning or dense urban regions. Civilian GPS devices can imitated by GPS satellite simulators that can produce false satellite radio signals which are powerful than original signals coming from the satellites. Most receivers of GPS can be acted unwisely while receiving the stronger signals and not responding to the weaker authenticate signals or ignoring them. Small changes of software to the GPS receivers will be affected by spoofing attacks Ultra sound positioning [6] systems can be operated by measuring the Time of Flight (ToF) of the sound signals that are measured between two sensor nodes. And the limitation of these systems is that is because of outdoor interferences they mainly used in outdoors. These types of systems are vulnerable to reduction of distance and enlargement of distance attacks by internal and external attacks.

Verifiable Multilateration (VM) [7] is one technique through which nodes can be securely positioned. Multilateration is a technique for position determining of devices, whose position are known based upon ranges between the devices and reference points that are measured. In VM proposes secure position verification will be done.

III. ATTACKS

Most probably, the probability of attacks within wireless sensor networks is higher when compared to networks, such as wireless LANs. The attacks can be distinguished as internal attacks and external attacks. In external attacks [16, 17] the attacker sensor node is not an authorized node of sensor network. External attacks can be further classified into active and passive attacks. Passive attack [17] involves unauthorized listening to the packets which are routed. In this type of attack can be done by methods of security, like encryption. External active attacks interrupt the functionality of network by introducing Denial-of-service attacks, like power exhaustion, jamming etc. Compromise of nodes is one of major problem that gives scope to the insider attacks. In insider attack node acts as an authorized participant and acts like a legitimate node. Eaves dropping: It is a type of attack in which capturing the sensitive data transmitted by other nodes such as passwords or any confidential information. False Data injection: It is attack in which insider nodes injects false data into network causing wastage of energy. Data drop: In this attack the insider nodes drops legitimate information which needs to be forward to the destination. Denial-of-Service attack: In this type of attacks the attacker tries to consume the available resources by sending extra information and thus preventing usage of resources to the legitimate resources: Selective forwarding attack: In WSNs all the nodes of the network will forward the data or messages that they receive to the other nodes. In this attack the attacker can create false nodes or take control over nodes in which nodes selectively forwards only some messages and simply drop other messages.

IV. DATA ORGANISATION

Previously in WSNs the communication pattern defined is hop-by-hop manner and these patterns are vulnerable to many types of insider and outsider attacks. Further the most of the existing patterns are end-to-end manner and there is need to overcome such type of vulnerabilities [1]. In sensor networks data is transferred from one to node another node. In simple applications data can be transferred from one node to another in one-to-one manner. But in huge networks the traffic pattern is one-to-many or many-to-one, where sensor nodes send data to one or more nodes. So, similar packets can be aggregated from multiple nodes in order to reduce the number of transmissions [8, 10]. Data aggregation is a combination of data from different servers that has done from certain techniques. In processing of network such duplicate elimination, data aggregation; compression is important in order to achieve efficiency of energy and optimization of data transfer. Security protocols may be hop-by-hop or end-to-end both each having their own encryption schemes taking in account different primitives. For data aggregation schemes introduces the concept of aggregated sensor nodes. An aggregator node can sense its own data while aggregating results that are received from children nodes and they can be leaf nodes or aggregators as well. Aggregator sensor nodes assumed to be multi-hop WSNs consisting of resource constrained or aggregated nodes [11] connected in tree topology. In [15] how the data gathering and security measure should be taken in homogeneous, heterogeneous networks are well defined. And in [10] introduces a novel secure data aggregation framework for WSNs which ensures the accuracy of data aggregation without effecting energy efficiency even if some or more number of aggregated nodes or sensor nodes is compromised.

V. SECURITY OBJECTIVES

The wireless sensor networks are deployed in mission critical system like military surveillance and in such systems security is more important. The security paradigms should ensure data authentication, data confidentiality and data availability

A. Data Authentication:

Data Authentication [1, 2] should ensure the node identity that is communicating from one node to another node, that is, a false node or compromised node cannot mask as a trusted network node.

B. Data Confidentiality:

Data Confidentiality [9] should ensure that a message sent is to be understood only by the intended recipient. IN WSNs data can be varied depending upon different applications. The data sent from event happening area to destination through number of nodes. As the communication range of sensor nodes is minimum, the data should be passed through number of intermediate nodes before finally reaching the sink. As long as the nodes are not compromised or attacked the confidentiality of the data should not be compromised or modified due to other compromised nodes along the path including intermediate nodes.

C. Data Availability:

This should ensure that the desired services of network are available even after the existence of denial-of-service attacks. As compromised nodes exists in Wireless sensor networks, it is important to protect data availability. So, security designs should be robust even if more no of compromised nodes exists. In processing of network false data removal is important in order to save the resources of network and to increase the network life time. Any security designs in WSNs should be resilient against denial-of service attacks such as report disruption [12] and selective forwarding attacks [13] where compromised nodes wontedly drops the packets by taking the advantage of false routing policies. In a Wireless sensor environment these security objectives should be achieved in order to protect the keying information so that attackers cannot take control over sensor nodes and misuse the network resources.

VI. KEY MANAGEMENT SCHEMES

To achieve security in WSNs, it is important to perform different cryptographic operations including encryption [6, 9, 22], decryption. Keys for cryptographic schemes for nodes are set up earlier so that information exchange can be done securely. Key management schemes are used to establish and distribute different types of cryptographic keys in the network such as individual keys, pairwise keys, group keys [3, 21]. A key management scheme should be made such that they should achieve the security objectives. The cryptography for the schemes can be symmetric or asymmetric. There are different types of key management schemes such as trusted server, self enforcing, key predistribution etc [3, 7, 21].

- The trusted server is a symmetric key distribution which is based on key distribution center i.e., it is the one which takes care of distributing the keys. Here the drawback is if server is compromised the network is totally compromised.
- The self enforcing is an asymmetric cryptography and is a good choice when a node is compromised reveals no security information about other keys in network except current ongoing keys. But having limited computation and energy resources of sensor nodes makes it undesirable.
- In key pre-distribution scheme all key information is distribute among all sensor nodes before deployment. The research on sensor networks suggests that pre-distribution schemes are most prominent.
- The public key scheme has been considered too expensive for small sensor nodes since public key algorithms require extensive computation and these sensors are not suitable for small sensors.

VII. MECHANISMS TO PROVIDE SECURITY OBJECTIVES

Interleaved hop-by-hop Authentication (IHA) [4] is one of the early techniques for providing data authentication in WSNs. In This technique all the sensor nodes are organized as clusters. For every cluster there will be one head which takes care of everything in cluster. That is, it will be responsible for receiving the packets, collecting reports and forwarding them to other nodes in order to send them to sink. The authenticity of every node is verified by using Message Authentication Codes (MAC) values. The data or report will be dropped if the node having unverified or altered MAC. Thus in IHA the false or compromised nodes are responsible for dropping the message. And IHA does not provide any mechanism for recovering this problem, and moreover it introduces communication overhead Another technique is statistical e-route Filtering (SEF) [12] for providing data Authentication and removing false injecting data. In this technique every sensor node is predistributed with keys for providing authentication after the node deployment. Because of this every sensor node is required to store keys for providing security objectives. Thus SEF suffers from storage overhead. And also these schemes suffer from threshold property. In these schemes compromising more number of nodes will lead to the breakdown of the whole network.

Location awareness is considered as basic requirement for sensor nodes, since sending the data is associated with the locations where the data is generated. Gligor and Eschenauer [7] proposed a probabilistic predistribution scheme for pair wise key establishment. The main idea is to make each sensor node to choose randomly set of keys from a pool prior to the deployment such that any two sensor nodes have some probability to share at least one key in common. Chan has extended this idea further and developed q-composite key predistribution, two key predistribution technique and random pairwise schemes. Both schemes have improvement over probabilistic predistribution scheme. However these schemes suffer from threshold problem. As the number of compromised nodes increases the number of pairwise keys affected also increases. Then [1] comes with a location based property for solving security objectives in WSNs. Location awareness is considered as basic requirement for sensor nodes, since sending the data is associated with the locations where the data is generated. Here the process comes as first they will divide the target terrain into geographic virtual grid [6, 7] consist of multiple cells. In this each node stores three types of keys 1. Unique secret key that is only shared between the sink and source and with this it able to provide node-to-sink authentication. 2. Cell key is shared between nodes that are in the same cells in order to provide data confidentiality and 3. A set of authentication keys shared in the data forwarding path and is to provide cell-to-cell authentication. To achieve the data authenticity a report carries Message Authentication Code (MAC) that is verified by the every node in the intermediate cells in the route forwarding path. For data availability the current node in the cell in route forwarding path collaborates with the next cell to inform that a valid report is dropped by the compromised node. To overcome the previous discussed threshold property this scheme uses a predefined secret sharing scheme. This scheme is well defined to provide all end-to-end data security mechanisms. But in every phase it has to communicate with every node and which is a communication overhead. The [2] uses a grid concept and location based pairwise key management scheme. It overcomes the threshold problem and provided it uses MACs to provide data authentication. But this method concentrates more on data authenticity and not on data confidentiality and data availability. The LNCS [2] is also a location based mechanism which employs a random network coding scheme and this scheme provides better data availability when compared to other schemes. Here it uses a hash tree to generate authentication information and apply authenticity test for finding the false data and the data which fails the test will be considered as false data and dropped. Sink is the final entity to rebuild the original message that is how it provides better data availability. It also better deals with the data authenticity and confidentiality. The coefficient matrices that are provided for report generation are expensive. Finally this method provides all security objectives but it is more expensive when compared to other schemes. However all these schemes energy consuming. Data aggregation plays important role in reducing the energy transmission and redundant data in large scale wireless sensor networks. The aggregation schemes can be end-to-end aggregation and hop-by-hop aggregation [14]. The end-to-end aggregation data aggregation introduces maximum data security with in-efficient aggregation of data and more likely to be vulnerable to active attacks, where as hop-by-hop data aggregation introduces maximum data integrity with efficient aggregation of data and are vulnerable to passive attacks. In data aggregation scheme rather than sending data of each sensor nodes to sink, a sensor node called data aggregator collects the data from other nodes and sends the aggregated data to the sink. The security issues such as data confidentiality, integrity and freshness of data becomes critical when WSN deployed in hostile environment where node nodes are subjected to compromise and failures. In general in aggregated data sending, first data is encrypted by the sensing nodes and decrypt by aggregator nodes, then aggregator nodes performs aggregation of the data and then encrypt the result, finally sink node decrypts the result. The hop-by-hop secure data aggregation can't provide data confidentiality at data aggregators and result is more overhead due to encryption and decryption process. To overcome these limitations end-to-end secure data aggregation are proposed. The end-to-end protocols perform data aggregation without doing decryption at the aggregator nodes. In a protocol called CDA proposed end-to-end privacy. This protocol uses additive and multiplicative encryption schemes that allow aggregators to aggregate encrypted data. This process is very expensive and adds data overhead and power consumption. The problem in previous end-to-end aggregator mechanisms is, it requires sending the information of non responding nodes. And data received at aggregator is encrypted by all the nodes. Then encrypted data at sink node is able to decrypt the data using the information of non responding nodes that is sent with the encrypted text. This process increases the number of bits transmitted with the encrypted data. To overcome this problem a protocol called SEEDA is introduced. In SEEDA the nodes are organized as tree structure [11]. In SEEDA (Secure End-to-End Data Aggregation) protocol rather than sending the information of non responding nodes they compute the encrypted data for non responding nodes considering them as 0. The encrypted data received by sink was added by all keys of sensor nodes even some of the nodes not respond. The sink node gets the aggregated data by subtracting respective keys of all sensor nodes. This process will reduce the number of bits transmitted because no additional information of non responding nodes is sent. This scheme adopts the best features of both hop-by-hop and end-to-end aggregation scheme. This scheme deals only to reduce the energy consumption and it does not deals with security objectives like what happens if the aggregator compromises. It considers only the non responding nodes but not explained what happens when having compromised nodes. Nabila and Mourad come up with security frame work that deals with the compromise of aggregators and data filtering process. The frame work ensures the accuracy of data aggregation without neglecting the efficiency of energy if some of the sensor nodes are compromised or all aggregator nodes are compromised. Most of frameworks define for aggregation process if they find compromise of aggregator or if Base Stations find malicious node they will totally reject the aggregation process resulting in the wastage of bandwidth and unnecessary resource consumption. The frame work defined in [10] overcomes the total aggregation rejecting process and ensures the data confidentiality. This frame work uses a two level hierarchical monitoring which verifies the integrity and accuracy of aggregated results. It deals with the pairwise key with each of its nodes and cluster heads and aggregator nodes thus providing data authenticity and data confidentiality between every node. It is resilient against false data injection attack, false aggregation attack and false data rejection and thus providing better data availability.

VIII. CONCLUSION

WSNs is growing rapidly day by day, and it has been using in many application where data is important, however security issues such as data authenticity, data confidentiality and data availability is challenging. We survey in WSNs how the data can be organized, what are the attacks, and how counter measures can be taken with the help key manage management schemes and have given what the schemes lack.

REFERENCES

[1] Kui Ren, Wenjing Lou, Yanchao Zhang," LEDS: Providing Location Aware End-to-End Data Security in Wireless Sensor Networks", IEEE 2008.

[2] Cungang Yang and Jie Xiao, "Location Based Pairwise Key Establishment and Data Authentication for Wireless Sensor Networks", IEEE 2006.

[3] W.Zhang and G.Cao, "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-Based Approach", Proc.IEEE INFOCOM, 2005.

[4] S.Zhu, S.Setia, P.Ning,"An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks", IEEE 2004

[5] S.Capkun and J.P.Hubaux,"Secure Positioning in Wireless Networks", IEEE 2006.

[6] Elai ne Shi and Adrian Perrig,"Designing Secure Sensor Networks", IEEE 2004.

[7] L. Eschenauer and V. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02), 2002.

[8] Poornima and Amberker, "SEEDA: Secure End-to- End Data Aggregation in Wireless Sensor Networks" 2010.

[9] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, pp. 103-105, Oct. 2003.

[10] Nabila and Mourad, "Adaptive Security level for Data Aggregation in Wireless Sensor Networks", ISWPC 2010.

[11] C. Castelluccia, C-F Chan, E. Mykletun, G. Tsudik, Efficient Provably secure Aggregation of encrypted data in wireless sensor networks, ACM Transactions on Sensor Networks, vol. 5, No.3, May 2009.

[12] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. ACM MobiHoc, 2005.

[13] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad- Hoc Networks, vol. 1, no. 2, 2003.

[14] Mlain; Aly, S.A, “Secure hop-by-hop Aggregation of End-to-end concealed data in Wireless Sensor Networks”, INFOCOM Workshop 2008, IEEE.

[15] Nakayama, H.; Ansari, N.; Jamalipour.; Nemoto, Y.;Kato, N.; “On Data Gathering and Security in Wireless Sensor Networks”, IEEE 2007.

[16] Y.Wang, Garhan Attebury, B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks”, VOL 8, 2006.

[17] Teodor-Grigolerupy, “Main Types of Attacks in Wireless Sensor Networks”, ISN 1790-5109.

[18] Sameer Tilak, Nael B. Abu-Ghazaleh, Wendi Heinzelman," A Taxonomy of Wireless Micro-Sensor Network Models"

[19] Chi-Fu Huang, Yu-Chee Tseng," The Coverage Problem in a Wireless Sensor Network" Copyright 2003 ACM 1-58113-764-8/03/0009