8th International Conference on Multidisciplinary Research
Osmania University Centre for International Program, Osmania University Campus, Hyderabad (India)
Conference World
6th-7th September 2019 www.conferenceworld.in ISBN : 978-81-941721-5-4

Different Data Security technique for Wireless Sensor Network

Piyush Raja[1], Dr. M. M. Rahman[2]

[1]*Research Scholar, Institute of Information Science & IT, M.U.Bodh-Gaya, Gaya, Bihar, India*
[2]*Associate Professor, PG Deptt. of Mathematics, A.N. College, Patna, Bihar, India*

Abstract

Wireless sensor networks (WSNs) have attracted a lot of interest over the last decade in wireless and mobile computing research community. An application of wireless sensor networks is frequent and rising, which range from indoor deployment scenarios in the home and office to outdoor operation in adversary's region in a tactical battleground. Wireless sensor networks have recently concerned a lot of interest to the researchers. However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network security. Whereas the set of challenges in sensor networks are diverse, we focus on security of Wireless Sensor Network.

Keywords: WSNs, WSNs Security, WSNs Attacks, WSNs Preventions and Detection.

I. Introduction

Wireless Sensor Networks (WSNs) are rapidly gaining interests of researchers from academia, industry and defense. WSNs consist of a large number of sensor nodes and a few sink nodes deployed in the field to gather information about the state of physical world and transmit it to interested users, typically used in applications, such as, habitat monitoring, military surveillance, environment sensing and health monitoring. Sensor nodes have limited resources in term of processing power, battery power, and data storage. Nodes in WSNs are passive, which can only monitor the events of interest and thus they are unable to react in the environment. Sensor nodes use wireless interfaces for communication and have short range due to limited energy [1].The sensor nodes have capabilities of self organization; there exist a complete coordination and cooperation among these nodes, which is the most important feature of these networks. Wireless sensor networks are mostly used for real time data processing in critical military operations, environmental monitoring, safety and protection of domestic infrastructure and resources. There are certain inherit limitations of these networks like lower batter power, low memory and band width [1][2]. Figure 1 presented a simple scenario of wireless sensor networks.

ISBN : 978-81-941721-5-4

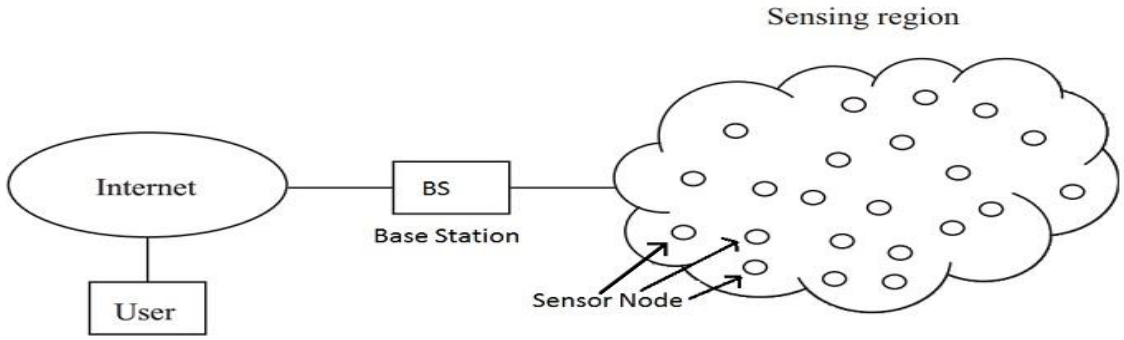

Figure: 1. Architecture of wireless sensor networks.

Due to these weaknesses conventional security techniques are not suitable and efficient for wireless sensor networks. Some researchers are also working for growth of a trust model for this purpose which may increase computation capabilities and decrease energy and storage utilization [3] [4]. As put side by side to wire networks wireless networks are more prone to attacks. There may be many types of attacks where the attacker fully destroy any network or inject/alter data in the middle. In many scenarios like emergency operation, natural disasters or battle field monitoring we cannot compromise on security because any negligence can cause a huge destruction. Therefore it is important to analyze these security attacks, security requirements and various approaches used to control these attacks [5] [6] [7].This paper evaluates different security requirements for wireless sensor networks, security attacks and proposed protocols by different researchers to control these attacks. The residue of the paper is organized as follows. In part II we have discuss about previous research paper for wireless senor networks. Part III describes various possible attacks in WSN. Part IV discusses different techniques for detection and prevention of various security attacks. Part V which is the last section of this paper has conclusion and future work.

II. Literature Review

In [8], implementing an encryption algorithm by using AES (Advanced Encryption Standard) has been proposed to provide for data confidentiality in a wireless sensor network. It focused on an AES-based symmetric key approach that shares the same key for encryption and decryption between both sides of communication. This algorithm results in plaintext by calculating 10 rounds mathematically to produce the ciphertext in a short period of time. In [9], a protocol based on public key cryptography for external agent authentication and session key establishment has been proposed. An external agent communicates through a public key encryption technique with a base station, which communicates with sensor nodes through sharing of a private key. The process for this protocol is broken down into three phases: registration, authentication and session key establishment. According to [10], an efficient cryptographic

approach for data security in WSNs using the Modern Encryption Standard Version-II is introduced. MES V-II proposes a type of symmetric key encryption. This algorithm, developed by Nath et al., uses the TTJSA and DJSA algorithms in a randomised method. In this approach, a generalised and modified Vernam cipher method is used with different block sizes and keys for each block. As an additional security criterion for this algorithm, feedback is also added to this method. After the direct stage encryption is completed, the entire file is divided into two interchanged parts and the modified Vernam cipher method with feedback and a new key will be repeated. Repeating this entire operation a number of times results in a system that is highly secure. In [11], the important factors and some of the security attacks were highlighted with an overview of security solutions to establish a secure infrastructure for WSNs. This began with the following security requirements:

• **Data Authentication:** message authentication is a critical dimension for sensor networks. This refers to the ability of each communication host to verify the other's identity.

• **Integrity:** this focuses on the correctness of the data to ensure that no changes are made by adding, altering or deleting information during the transmission.

• **Data Confidentiality:** this ensures that any message is known by the sender and receiver only. The standard approach for achieving this requires use of encryption techniques.

• **Availability:** this ensures that data is available at all times or at the time of any request. Some security attacks such as denial of service will affect data availability, but weak network designs and security mechanisms can also result in unavailability of data. Protecting availability requires avoiding a single point of failure in the design phase for any system, as well as avoiding computation-heavy algorithms that lead to energy consumption of the sensor nodes.

• **Data Freshness:** this ensures that no old messages have been replayed by a malicious actor. Timestamps can be applied to achieve this goal. In addition, the following terms are used to describe wireless sensor attacks:

• **Denial of Service (DoS):** this type of attack aims to reduce network bandwidth and paralyse resources. Such attacks on WSNs can appear as various types placed in different network layers.

• **Sybil Attack:** this type of attack subverts a reputation system by falsifying identities.

• **Blackhole/Sinkhole Attack:** in this type of attack, a malicious node acts as a black hole that controls the traffic of WSNs. This occurs when a malicious device is introduced between any two nodes and controls communication between them.

• **Wormhole Attack**: in this type of attack, network packets at one location in the network are tunneled through to another location in the network. Retransmissions are then returned to the start location.
Finally, the literature review focused on some WSN security solutions such as the following:
• **Shared Keys:** this is a normal protection schema that provides the same key for both encryption and decryption schema.

• **Protected Grouping:** this involves a large number of sensor nodes in a WSN in which some nodes are grouped together to complete specific tasks.

• **Encryption:** this involves applying different cryptographic approaches such as message authentication codes, symmetric keys and public key encryption.

• **Secure Data Aggregation**: sensor nodes typically gather information in order to transmit it to the base station. To reduce the energy consumed by sensor nodes, this information should be aggregated at an intermediate sensor level by using an appropriate aggregation function.

• **Security Protocols for Sensor Networks (SPINS):** this is a group of various security building blocks designed to achieve different security requirements.

• **Link Layer Security Architecture (TinySec):** this is a tiny security package installed in the applications of a sensor network. It is a part of the official release of TinyOS. Its security preferences are authentication encryption (TinySecAE) and authentication only (TinySecAuth).
In [12], a multilevel security mechanism is introduced by using a data-oriented random number generator to encrypt a tag of frames. The first level will be started with a interleaving method. Second, the value of a pseudo-random number generator is seeded. Third, a number bank is distributed initially. The final level is started by applying operations to the number bank. In [13], a cryptographic schema using chaotic map and genetic operations has been suggested for WSNs. It integrates the advantages of the elliptic curve method, chaotic map and genetic encryption to achieve data confidentiality. There are three phases to form the proposed block cipher as follows:
• Key Establishment Phase: after the random selection of a secret key from the key pool, sending and receiving nodes interchange it between them. This phase will use the elliptic curve method based on a prime field to produce a large key pool for node authentication.
• Generation of Pseudorandom Bit Sequence: in this phase, pseudorandom bit sequences are produced by using chaotic map functions.
• The Encryption Process: confusion and diffusion are the main concepts used to help design a block cipher. To achieve confusion, an obscuring relationship between the ciphertext and the symmetric key must be applied. Diffusion, on the other hand, is achieved by scattering the repetition of the plaintext by

ISBN : 978-81-941721-5-4

spreading it over the ciphertext. Three different operations can be implemented by this cryptographic technique: XOR, mutation and crossover.

In [14], a flooding method routing technique is introduced that depends on dummy data sources. The main idea behind this technique is that each node can be considered as a dummy data source that sends real data after sensing an event to the destination node; all of this node's neighbor nodes will receive dummy data. Although this approach has the advantage of making it difficult for an adversary to distinguish between the real packet and dummy ones, it leads to dummy traffic and power consumption as a result of this. A novel solution is proposed by using variablesized dummy packets. The dummy packets will differ in size from the real packets, thus saving energy; however, an adversary will still find it difficult to distinguish the real packet from the dummy ones. In [15], a solution is proposed for catching malicious nodes with trust support in WSNs (CMNTS); this targets specific WSN attacks by malicious node, including packet modification, packet dropping, Sybil Attack, packet misrouting and bad-mouthing attack. CMNTS initiates the process by creating a parent-child tree contains related information in a sink node. The data is transmitted in multiple rounds with the same time duration for each round. The parent is selected by its node. CMNTS detects bad nodes after each round. In [16], a honeypot framework for WSNs is introduced. This is based on a technique that uses a decoy system or server to attract an attacker. This technique will gather information about the attacker's behaviour and use this to identify weaknesses and vulnerabilities so these can be resolved them from a design and security perspective

III. Attacks In Wireless Sensor Networks

In this part we talk about different types of attacks and their affects in Wireless Sensor Networks. There are two major types of attacks in wireless sensor networks.

A. Active Attacks These is such types of attacks in which the attacker cause destruction. There is physical damage in the network like destruction of resources, alteration of data, changing traffic direction or stoppage of data to sink nodes. These attacks are easily identifiable and we can stop the attackers as well as start the system recovery process.

B. Passive Attacks These are another types of attacks in which the attackers only observe different activities on the network check confidential information but don't cause any physical destruction or any alteration of information. However the passive attackers can launch active attacks and cause a big damage because during observation of different activities on the network he is able to find weak points and clues in the network and wait for a suitable time to launch an attack. Passive attacks are more dangerous as compare to active attacks because in passive attacks you are unable to recognize your attacker.

C. Flood Attacks Karlof et al [17] in 2003 introduced a flood attack in wireless sensor networks. For this purpose Hello packets are used to destroy the network resources. In this attack the attacker floods Hello messages in the network that are dispersed in the whole network. However the attacker pretended that the sender of the packet is in their neighbour, therefore when the sender node want to send any sensed information to a sink node then they forward it toward attacker node. Because they think that the attacker node is in their neighbour, and so any information forwarded toward base station in those packets can be easily accessible to attacker.

D. Black hole Attack Culpepper et al [18] identified a new attack in wireless sensor networks that is called black hole attacks. In such type of attacks the attacker nodes act like a black hole, where the attacker node listen the route request packets from its neighbours and reply them back using fake information about shortest route toward sink node. So every node in its surrounding set the attacker as a next node for data forwarding toward sink. Any node which wants to send data to a base station will forward it towards attacker. This provides the attacker with an opportunity to analyze these packets and extract important information.

E. Black ert et al [19] launched a new attack in wireless sensor networks. The main objective of this attack is to waste the available resources of the network. In this attack the attacker (malicious node) send extra packets in the network without any need and keep the route as well as the base station busy. So the authentic users are unable to send data, access resources and get services.DoS attack is launched to prevent the legitimate users of the network from utilization of resources to get any service. DoS attack may vary from layer to layer in OSI model. At physical layer DoS attack may be in the form of traffic blockage and delay, at data link layer it may cause collision of frames and unfairness. DoS attack at network layer may be packet routing in wrong direction as well as black holes creation. While on transport layer DoS attack may be flooding (extra traffic) or desynchronization of data in the network [20] [21].

F. Sybil Attack Wireless sensor networks are more vulnerable to sybil attack. In such types of attack a node changes its ID continuously and attacker nodes using multiple identities of the legitimate sensor nodes at the same time. Main purpose of this attack is to increase the resource utilization and decrease data integrity. Sybil attacks mostly happened in distributed systems on network servers for data aggregation. Although detection of such nodes that launches Sybil attacks is a very hard task. Dovcevr et al [22] proved that Sybil attacks can be controlled however in the absence of centralized controller there are more chances of Sybil attack. Therefore in wireless sensor networks we have a centralized base station which helps in prevention of Sybil attacks. Many others like Newsome et al [23] detect Sybil nodes in the network with the help of radio resources and also calculate the probability of a Sybil node in the network.

G. Information Alteration Sensor nodes have responsibility to sense an event from its physical world and transfer that information toward a base station [24]. However in the middle of communication there is chance of spoofing data by an attacker, so he may alter the complete message or a part of it to misguide the base station. In this attack the attacker can observe all the traffic inside the network that's why if the attacker node did any alteration, we can identify it and detect the attack. However if he is only observing all the activities and ask someone else to attack then it is very difficult to detect such attackers.

H. Worm holes In this attack the whole traffic of the network is tunnelled in a particular direction at a distant place, which causes deprivation of data receiving in other parts of the network. Sometime any information which is very important and should be deliver to the base station in specific time is sended toward worm hole [25].

I. Looping In this attack few nodes in the network cause the circulation of data in a particular region. This attack stops data to send to a destination node and revolve in the same region which increase network traffic as well as causes latency [25].

J. Node Replication In this attack the attacker add a new sensor node in the network, which is using the ID of a legitimate user. This attacker node replication can cause a big destruction in network because he can attack any node or sink node by pretending himself as a legitimate user. Once the replicated node is able to access the network then there is possibility that he may get the position of a strategic node or the security keys may be exposed [26].

IV. Prevention And Detection of Various Security Attacks

In this part we talk about that how to prevent and detect different security attacks in wireless sensor networks. There are many techniques with the help of which we can protect our network from different attacks like DoS attack, Spoofing, data aggregation, secure routing, intrusion detection and prevention.

A. Denial of Service Attack (DOS) For Denial of service attack on transport layer the base station always force the sensor node to request more resources up front then the server and jamme the traffic [27]. Defending against jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion [28]. There are two phases in which the sensor nodes near the jammed region report their status to their directly connected neighbors, who then collaboratively define the jammed region and simply route it onward. Protection against Network IDs, as well as physical protection of whole network is necessary to prevent DoS attack.

B. Sybil Attack To control Sybil attack we have to change session key after specific time as well as reconfiguration of network devices. Physical protection of the network is also very important for prevention as well as detection of such attacks.

C. Wormhole For prevention of wormhole attack there should be an efficient monitoring system that should monitor all the network devices. The monitoring system may use packet leaches for this purpose.

D. Spoofing and traffic Analysis For detection and prevention of spoofing attacks regular monitoring of sensor nodes as well as sending of dummy packets when there is no traffic on the network. Another option is to use different routes to send confidential information.

E. Detection of Node Replication B. Prano et al [26] proposed two techniques for detection of node replication in wireless sensor networks. i) Line selected multicast and ii) Randomized multicast. These techniques take the advantage of node broadcasting, where a sensor node propagates a broadcast message in the network. If a node receives a duplicate message it identifies the conflict and recognizes the duplicate node. Randomized multicast randomly chooses the two witnesses for replicated node, as compare to line selected multicast. However randomized multicast has more communication overhead.

F. Intrusion Detection As compared to other attacks, intrusion detection is based on behavior of intruders. Detection of this attack is possible when intruder node start abnormal behavior as compare to normal sensor node. For this purpose the base station maintain a record of intruder signature and is able to identify an attacker and legitimate node.

G. Trust between Nodes In such type of networks there may be certain level of trust, because traditional security techniques are not possible to implement in these networks due to limited energy, memory and computation power. Many authors proposed trust management techniques in these networks like H. Zahu et al [33] compute certain level of trust in wireless networks between different nodes. For this purpose they used authenticated transitive graph and transitive signature scheme. P. Zhang et al [28] developed a trust based security system for secure routing and data protection.

V. Conclusion and Future Work

Wireless sensor Networks have certain inherit limitations therefore instead of statement security it also desires a fool proof physical security. Most common attack in such type of network is that node compromise to accept tempered information and forward it onward. Therefore cryptography is not enough to secure such networks. Sensor nodes confirmation and encryption of information may make it more strengthened. In this paper we discussed security requirement for wireless sensor networks, we consider different security threats and possible attacks as well as existing security approaches proposed by different researches with their basic characteristics. Our future work we have discussed about more relevant security protocol and more securities for wireless sensor network.

Reference

[1] N. Boudriga, A new scheme for mobility, sensing and security management in WSB" IEEE Annual simulation symposium (ANSS), 2006.
[2] J. Albath, S. Madaria, Practical Algorithms for Data Security (PADS) in wireless sensor networks Mobi-De 07, Beijing, China 2007.
[3] N. D. Vasumathyl, G. Velmathil, N.SkalavosII, On the Rijndael Encryption Algorithm Matalb Based implementation Department of Electronics and Communication Engineering, Sirsiva Subramania Nadar college of Engineering Tamalnadu, India, 2008.
[4] www.wikipedia.com ttp://en.wikipedia.org/wiki/Advanced Encryption Standard, Jan 2009.
[5] L. Tobarra, D. Cazorla, F. Cuartero, Formal Analysis of Sensor Network Encryption Protocol (SNEP) IEEE Internatonal Conference on Mobile Ad-hoc and Sensor Systems, MASS 2007, PISA, 8-11 Oct. 2007.
[6] S. Zhu, S. Setia, S. Jajodia, LEAP, Efficient Security Mechanism For Large Scale Distributed sensor Networks Proceeding of ACM Conference on Computer and Communication Security, (CSS,03) pp,6272, 2003.
[7] M. Sherin. M. Yousef, A. Baith. Mohamd, mark A. Mikial, An Enhanced Security Architecture For Wireless Sensor Network Recent Advances on Data Networks, Communications, Computers, ISBN-17905109, Sep 2009.
[8] Panda, M. Data security in wireless sensor networks via AES algorithm. in Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on. 2015. IEEE.
[9] Sekhar, V.C. and M. Sarvabhatla. Security in wireless sensor networks with public key techniques. in Computer Communication and Informatics (ICCCI), 2012 International Conference on. 2012. IEEE.
[10] Praveena, A. and S. Smys. Efficient cryptographic approach for data security in wireless sensor networks using MES VU. in Intelligent Systems and Control (ISCO), 2016 10th International Conference on. 2016. IEEE.

[11] Jain, A., K. Kant, and M. Tripathy. Security solutions for wireless sensor networks. in 2012 Second International Conference on Advanced Computing & Communication Technologies. 2012. IEEE.
[12] Navin, A.H., et al. Encrypted Tag by Using Data-Oriented Random Number Generator to Increase Security in Wireless Sensor Network. in Computational Intelligence and Communication Networks (CICN), 2010 International Conference on. 2010. IEEE.
[13] Biswas, K., V. Muthukkumarasamy, and K. Singh, An encryption scheme using chaotic map and genetic operations for wireless sensor networks. IEEE Sensors Journal, 2015. 15(5): p. 2801-2809.
[14] Celestine, J., et al. An energy efficient flooding protocol for enhanced security in Wireless Sensor Networks. in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island. 2015. IEEE.
[15] Prathap, U., P.D. Shenoy, and K. Venugopal. CMNTS: Catching malicious nodes with trust support in wireless sensor networks. in Region 10 Symposium (TENSYMP), 2016 IEEE. 2016. IEEE.
[16] Markert, J. and M. Massoth. Honeypot framework for wireless sensor networks. in Proceedings of International Conference on Advances in Mobile Computing & Multimedia. 2013. ACM.
[17] C. karlof, D. Wagner, Secure Routing in Wireless Sensor Networks, Attacks and Countermeasures Elsevier's Ad-hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, pp, 293315, September 2003.
[18] B.J. Culpepper, H.C. Tseng, Sink hole intrusion indicators in DSR MANET's Proceeding of International Conference Broad Band Networks. PP, 681-688, 2004.
[19] Blackrert, W.J. Gregg, D.M. Castner, A. k. Kyle, E.M. Home, Jokerst. R.M, Analyzing Interaction between Distributed Denial of service Attacks and Mitigation Technoologies Proceeding of International Conference information Survivability and Exposition, DARPA, pp, 2636, 22-24, April 2003.
[20] Wang. B.T, Schulzarinne.H, An IP Traceback Mechanism for Reflective DOS Attacks Canadian Conference on Electrical and Computer Engineering, pp, 901-904, 2-5, May 2004.
[21] Al-Sakib khan pathan, Hyung-Woo Lee, Choong Seon Hong, Security in Wireless Sensor Networks: Issues and Challenges International Conference ICACT-o6. 20-22 Feb, 2006.
[22] Douceur. J, The Sybil Attacks First International workshop on Peer to Peer Systems 2002.
[23] Newsome. J, Shi. E, Song. D, Perrig. A, The Sybil Attacks in sensor Networks Analysis and Defenses Proceeding of International Symposium on Information Processing in Sensor Networks, ACM, pp 269-268, 2004.
[24] Pfleeger C. P, Pleeger. S. L, security in Computing 3rd Edition Prentice Hall, 2003.
[25] Mona sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabdai, S. Beheshti "A Survey on Wireless Sensor Networks Security" International Conference Science of Electronics, Technologies of Information and Telecommunication, Tunisia, March 25-29, 2007.
[26] B. Parno, A. Perrig, V. Gligor, Distributed Detection of Node Replication Attacks in Sensor Networks Proceeding of IEEE Symposium on Security and Privacy, May 2005.
[27] H. Zhu, F. Bao, R.H.Deng, k. Kim Computing of Trust in Wireless Networks In proceeding of IEEE International Conference on Vehicular Technology, Los Angles, California, September 2004.
[28] Z. Yan, P. Zhang, T. Virtanen Trust Evaluation Based Security Solution in Ad-hoc Networks Proceeding of 7th Nordic Workshop on Secure IT System, 2003.