ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 3, March 2018

Emerging Security Issues and Challenges in Wireless Sensor Networks

Mandeep Kumar[1], Dr. Jahid Ali[2]

Research Scholar, Department of CSE, IKG PTU, Kapurthala, Punjab, India [1]

Professor & Director, Department of Computer Science, SSICMIT, Badhani, Pathankot, Punjab, India [2]

Abstract: Wireless Sensor Network (WSN) is a evolving technology that is using in various application areas like as military, video surveillance, automation of industry, connected smart homes, robot control, environmental, agriculture etc. In many applications, Wireless sensor networks are deployed very frequently, continuously and also these are increasing. The security issues, data confidentiality and integrity become an important point when sensors are deployed in a difficult conditions and environment. In this research paper I discussed about the security related issues and challenges in WSNs. We identify various attacks in WSN, review various security schemes proposed so far for the wireless sensor networks. The approach for improving the security of wireless sensor networks is also reviewed.

Keywords: Security, Attack, Challenge, Wireless Sensor Network, routing**.**

I. INTRODUCTION

Wireless Sensor Network is a collection or group of specially designed sensor nodes consist of transducers that having an infrastructure which can communicate to other sensor nodes. These sensor networks can be used for monitoring and even recording the events at diverse or hostile environment [1]. The main idea behind sensor network is to disperse the small sensor devices and these are capable to sensing as well as communicating with other sensor devices also. These days sensors can monitor temperature, pressure, humidity, soil makeup, traffic monitoring, noise levels, controlling and monitoring of air traffic and medical equipment, robot control, weather conditions and other properties [2]. The wireless sensors are used to have the communication among the sensor nodes in wireless sensor networks.

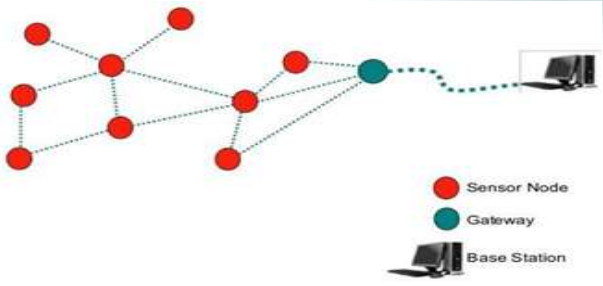

Fig. 1 Structure of WSN.

Wireless sensor networks have many attracted features and these features attracted many researchers to work in this field. Figure 1 shows the typical structure of WSN. As far as this field growing preference but still many security issues are still need to addressed. In this research paper, we are elaborating various security issues and challenges in the field of Wireless sensor networks and also discuss various parameters that need to be explore.

As the wireless sensor networks are growing rapidly so it required need to have effective security mechanisms and tools, because a sensor network has to deal with sensitive information and also it usually operate in hostile diverse unattended environments. Sensor devices are usually deployed in areas that present the risk of any physical attack. The major challenge faced by any sensor networks is size of sensors, the processing power, memory size and the tasks that are usually expected from the sensor devices. We discuss various issues and challenges in this research paper.

II. SECURITY IS COMPLEX IN WSN

Because of WSNs Characteristics:

- Anti-jamming and physical temper proofing are Impossible
- Greater design complexity and energy consumption Denial-of-service (DoS) attack is difficult
- Sensor node constraints
  Sensor nodes are susceptible to physical capture

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 3, March 2018

- Deploying in hostile environment.
  Eavesdropping and injecting malicious message are easy
- Using wireless communication
  Maximization of security level is challenging
- Resource consumption
  asymmetric cryptography is often too expensive
- Node constraints
  centralized security solutions are big issue
- No central control and constraints, e.g. small memory capacity.
- Cost Issues
  Overall cost of WSN should be as low as possible.

III. SECURITY ISSUES AND CHALLENGES

The wireless sensor network usually have limited processing power, limited storage capacity, limited communication bandwidth, limited energy and even limited size of hardware. The communication cost is also higher. The communication cost from one sensor node to other node is very costly as compared to the instructions processing and computations. Following are the major issues and challenges faced by WSNs.

A. Limited Memory Space

The sensor device is actually a small electronic device having a small memory and CPU. The memory is usually ranges from 2KB to 256KB. The messages in WSNs have even a little size. There is even no understanding of division in different utilizations of wireless sensor networks [3]. For designing a powerful secure network it is also important to have code for the safety computation. But limited memory space required our network to use limited code.

B. Limited Power Energy

In WSNs the energy is consumed during sensing, communication between sensor nodes and microprocessor processing. The communication between sensor nodes is much costlier as compared to microprocessor processing. Also these sensor nodes are places in hostile environments and at disperse locations so this is also not possible to replace or recharge these batteries.

C. Unreliability

The sensor nodes operate in a wireless open medium, then any transmission can be easily attacked by malicious agent and cause jamming like issues. Conflicts can also occurred during colliding of packets. Packets can be damaged due to errors. This result in loss of packets.

D. Unattended Deployment

Sensor nodes can be deployed in areas which are unattended by human being. Thousands or millions of nodes can be deployed. So efficient requirement from security point of view is needed to address this sensor nodes which are dispersed.

E. Unfixed Infrastructure

The WSNs sensor nodes do not have any fixed infrastructure. Many sensor nodes generally get dead or replaced from their location causing the routing scheme to be changed. Further there is no central controller to monitor the sensor network. So a security mechanism must be implemented.

IV. SECURITY NEEDS

The main reason to provide security is wireless sensor networks is to give seamless services and protect the network resources from attackers. In this topic we discuss about major requirements like confidentiality, integrity and availability and this is the aim of any computer and network security.

A. Data Confidentiality

This means to prevent any untrusted party from accessing the secure data inside the network. It is also known as privacy of data. The main aim is that the secure data should not fall into hands of unintended users. The much better way to hide the data from unauthorised users is to encrypt it using secret key [4] [5]

B. Data Integrity

This means that the data should not modified in transmission. It is the guaranty that the information is accurate and true during transmission process.

C. Data Availability

This means that any authorised request should have access to the data, services and resources whenever it need. This request cannot be denied.

V. ATTACKS IN WSNS

A. Sybil Attack

In this type of attack, the attacker can make a multiple node copies of the legitimate node in the network. Thus, a

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 3, March 2018

single node now have multiple identities to other nodes in the network [6]. Figure 2 shows the Sybil Node S now having multiple identities with A, B and C.

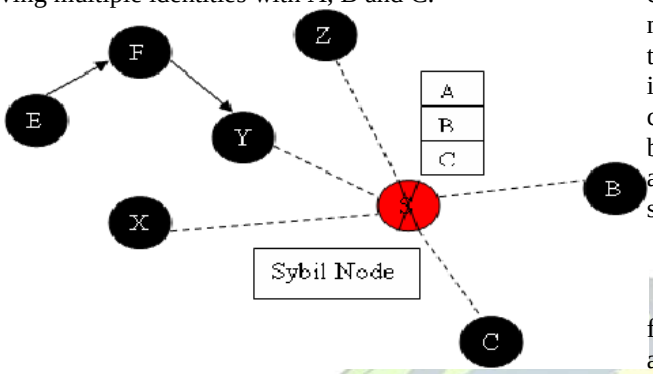

Fig 2. Sybil Node with multiple identities

The data integrity, security and network resources utilization decreases greatly with Sybil attack. One Solution the defend the Sybil Attack is Public Key Cryptography. But this scheme proved to be very expensive in a resource constrained network [5]. Newsome et. al [7] showed defence against Sybil attack by using radio resource testing and thereby detect the presence of any Sybil nodes in the sensor network.

B. Wormhole Attack

Wormhole attack is an attack in which the attacker captures the packets at one location in the network and tunnels those to another location [8] which distribute them locally. This can confuse the routing mechanisms which rely on the knowledge about distance between nodes. This type of attack does not even need compromising a node in the sensor network.

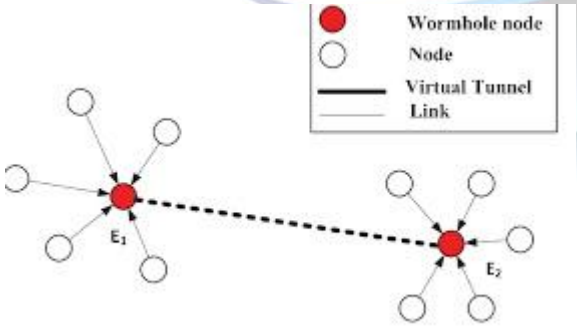

Fig. 3 Wormhole Attack

The wormhole attack is shown in figure 3, Malicious nodes E1 and E2 are connected by powerful connection, create a wormhole. Information will be record by the malicious node and then finally by the attacker [9]. Solution to these attacks include Directional Antenna approach [11] in which nodes use specific sectors of their antennas to communicate with each other. Other solution is Connectivity based approach [10], it needs connectivity information and also need tightly synchronized clocks. SAM [12] showed statistically calculation of relative frequency of path.

C. Denial of Service Attack

This type of attack can disturb the network traffic in the form of interference, noise or collision at the context of attacks [13]. The main aim of DoS attack is to drain out the resources in the network by transferring extra load to the system. Thus preventing the authorised users to access the services. Thus it destroy the network capability to provide the service [14]. The solution to prevent DoS attacks includes payment for network resources, pushback, strong authentication and identification of traffic [14].

D. HELLO Flooding Attack

In this type of attack, the attacker node which is not a legitimate node in the network, can flood HELLO request to legitimate nodes and thus break the overall security of the WSN. Actually WSN nodes uses hello messages to announce themselves to their neighbour's nodes. A node which receives these messages may assume that it is in the range of the sending node. But a laptop –class attacker node which is having high transmission power could convince every other node in the network that the attacker is its neighbour. Now all other nodes start responding to this HELLO message from the attacker node. Thus the legitimate nodes start wasting their energy. This results in a confusion inside the WSN [15]

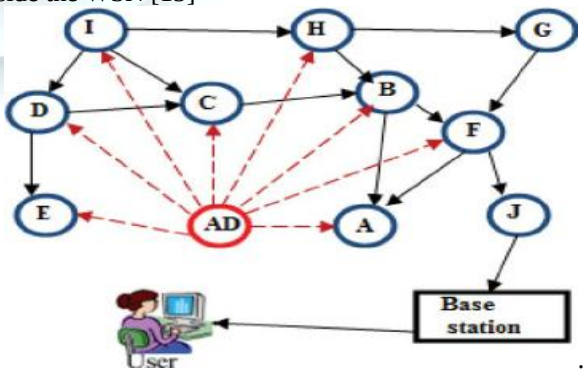

Fig. 4 Hello-Flood attack

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 3, March 2018

Figure 4 showed how a legitimate node now start considering adversary node as legal node and start responding to it. A. Hamid [16] showed a solution to Hallo-Flood Attack. They proposed a Multi-path Multi Base flooding technique in which a sensor node maintains a number of secret keys. And each base station also has all the secrets. Venkata C [17] also proposed a solution by using identity verification protocol. This protocol verifies the bi-directional link.

E. Sinkhole Attack

In this type of attack, the attacker compromise a node inside the network. Thereafter this compromise node try to attract all the traffic from neighbouring nodes based on routing information inside the routing protocol. The compromised node looks attractive to all the neighbouring nodes according to the routing algorithm. Further the laptop class attacker node has high transmission power that provide a high-quality route to reach a wide-area network. Figure 5 demonstrate this type of attack.

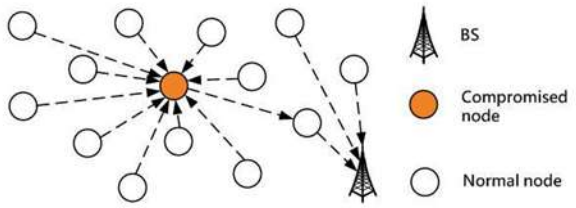

Fig. 5 Sinkhole attack using compromised node.

The solution provided in [18] as data consistency & network flow information approach which involves the base station in detection process. The base station asked the affected node to reply with their Ids and the Ids of next hop and associated cost.

VI. Research Issues In WSNs

Wireless Sensor networks are vulnerable to attacks due to the broadcast nature of the transmission medium. Further nodes are placed in hostile or dangerous environment where they are not physically protected. In this topic, various research issued related to the security of WSNs are discussed.

A. Research issues in Cryptography techniques for WSNs.

To achieve security in WSN, so for this network it is important to have cryptography techniques including encryption, authentication and so on. Asymmetric cryptography is very expensive for many applications, thus there is need for a promising approach to use more efficient symmetric cryptographic alternatives. But symmetric key cryptography is not as versatile as public key cryptography. Further applying any encryption schemes required transmission and processing of extra bits and hence it takes extra memory and battery power, which are very important resource for sensor life. Thus further research in this regard is needed which increases the lifetime of sensor nodes while using the encryption mechanisms also. Better key management schemes, better shared key discovery methods, study of node compromise distribution and integrating it in key management is the need.

B. Research issues in Secure Data Aggregation

Data aggregation is the process in which intermediary nodes called "aggregators" collect the data from sensor nodes, process it locally, and forward only the result to the end-user. This operator of aggregation reduces the amount of transmitted data and thus increases the lifetime of network. But because of the deployment environment, the aggregators can be compromised. The main defence against this threat is cryptographic mechanisms, integrity and confidentiality. Further research techniques are needed to ensure that users can still be confident of the accuracy of the aggregated data when the aggregator and sensor nodes are under the control of the adversary. New data aggregation protocols need to be developed to address higher scalability, processing overhead, communication overhead, and data compression rate. Secure, very efficient and cost effective data aggregation mechanisms need to be developed.

C. Research issues in Secure Group Management

In-network processing of data is performed in WSN by dividing the network into small groups and analyzing the data aggregated at the group leaders. So the group leader has to authenticate the data it is receiving from other nodes in the group. This requires group key management. However, addition or deletion of nodes from the group leads to more problems. Consequently, secure protocols for group management are required.

D. Research issues in Intrusion Detection

The problem of intrusion detection is very important in the case of WSNs. Traditional approaches which do an anomaly analysis of the network are very expensive in terms

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 3, March 2018

of network's memory and energy consumption. So there is need of decentralised intrusion detection. The proposed IDS protocols focus on filtering injected false information only. These protocols needs to be improved to address scalability issues.

E. Research issues in Secure Time Synchronization

Time synchronization is very important in WSNs due to collaborative nature of sensor nodes. It is required in many sensor network operations such as coordinated sensing tasks, sensor scheduling (sleep and wake) and data aggregation etc. However none of the time synchronization schemes were designed with security in mind. Hence, they are not suitable for applications in hostile environments.

F. Research issues in Secure Location Discovery

Secure location discovery play an important role in many sensor application such as environment monitoring and target tracking. Without any protection, an attacker can easily mislead the location estimation at sensor nodes and thus disturb the normal operations of the network and nodes will determine their locations incorrectly. Minimum Mean Square Estimation (MMSE) approach is used to deal with malicious attack against location discovery in WSNs. This used the voting based location estimation technique.

VII. CONCLUSION

Security is important for wireless sensor networks because these are deployed in hostile environments. Wireless communications employed by sensor networks facilitates eavesdropping and packet injection by an adversary. So it demands security for sensor networks at design time to ensure operation safely, secrecy of sensitive data, and privacy of people in sensor environments. But providing security in sensor networks is even more difficult than MANETs due to resource limitations of sensor nodes. WSNs are still under development, and many protocols designed so far for WSNs have not taken security into consideration. On the other hand, the salient features of WSNs make it very challenging to design strong security mechanisms and protocols while still maintaining low overheads. We summarize typical attacks on sensor networks. Many security issues in WSNs still remain open and I expect to see more research activities on these open research issues in the future.

ACKNOWLEDGMENT

My sincere thanks to my honorable guide Prof. Jahid Ali and others who have contributed towards the preparation of the paper.

REFERENCES

[1]. Iordanis Koutsopoulos and Maria Halkidi "Measurement Aggregation and Routing Techniques for Energy-Efficient Estimation in Wirless Sensor Networks," WiOpt 2010.

[2]. Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.

[3]. Said O. Amara, R. Beghdad and Mourad Oussalah, "Securing Wireless Sensor networks: A survey",Taylor & Francis, 04 feb 2013

[4]. Abhishek Jain, Kamal Kant, and M. R. Tripathy, "Security Solutions for Wireless Sensor Networks", to appear in IEEE ICACCT 2012.

[5]. Mayank Saraogi, "Security in Wireless Sensor Networks", University of Tennessee, Knoxville.

[6]. J. R. Douceur,(2002) "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems(IPTPS"02).

[7]. Newsome, J., Shi, E., Song, D, and Perrig, A, "The Sybil attack in sensor networks: analysis & defenses", Proc. of the third international Symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[8]. Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

[9]. David Martins, and Herve Guyennet, Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", 2010 IEEE.

[10]. Dong, D., Li, Z., Liu, Y., & Liao, X. (2009). Wormcircle: Connectivity-based wormhole detection in wireless ad hoc and sensor networks. Paper presented at the Parallel and Distributed Systems (ICPADS), 2009 15th International Conference.

[11]. Hu, L., & Evans, D. (2004). Using Directional Antennas to Prevent Wormhole Attacks. Paper presented at the NDSS.

[12]. Qian, L., Song, N., & Li, X. (2007). Detection of wormhole attacks in multi-path routed wireless ad hoc networks: a statistical analysis approach. Journal of Network and Computer Applications, 30(1), 308-330.

[13]. Y. Bevish Jinila, K. Komathy (2015), "Rough Set Based Fuzzy Scheme for Clustering and Cluster Head Selection in VANET", ELEKTRONIKA IR ELEKTROTECHNIKA, Vol.21, No.1, pp.54-59, ISSN : 1392-1215.

[14]. A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, 47(6):53– 57, June 2004.

[15]. David R. Raymond and Scott F. Midkiff, (2008) "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, val. 7, no. 1, 2008, pp. 74-81.

[16]. Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[17]. A Hamid, S Hong, (2006) Defense against Lap-top Class Attacker in Wireless Sensor Network, ICACT

[18]. Venkata C. Giruka, Mukesh Singhal, James Royalty,Srilekha Varanasi, (2006), Security in wireless networks,Wiley Inter Science.

[19]. Edith C. H. Ngai, Jiangchuan Liu and Michael R. Lyu; "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks" IEEE International Conference on Communications, 2006, Volume 8, pp. 3383.

BIOGRAPHY

Mandeep Kumar received B.Tech in CSE from Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India in 2003 and M.Tech in Computer Science and Engineering from Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, Punjab,India in 2013. Presently he is pursuing PhD from IKG PTU Kapurthala, Punjab. His research interest is in wireless sensor network. (mandeep_recj@yahoo.com).

Dr. Jahid Ali has vast research, teaching and administrative experience in SSGI Badhani, since 2002.He has specialized in Speech Recognition Technology, Artificial Intelligence, Advanced Data Structures, Applied Mathematical and Programming languages. He has published about 15 papers in National Journals of repute and guiding 4 Ph.D students from IKG PTU. He has been awarded full travel grant for presenting a research paper in University of Taxas, USA by All India Council for Technical Education (AICTE). (zahidsabri@rediffmail.com)