World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 1, No. 7,302-306, 2011

Approaches to Wireless Sensor Network: Security Protocols

Harmandeep Singh
Electronics & Communication Engineering
Guru Nanak Dev Engineering College, Ludhiana
Punjab, India

Garima Malik
Electronics & Communication Engineering Rayat
Bahra Inst.of Eng. & Nanotechnology
Punjab, India

Abstract- The advancement of electronics and wireless communication technologies have enabled the development of large scale wireless sensor network that consist of many low-power, low-cost and small size sensor nodes. With the help of sensor network we facilitate large scale and real time data processing even in complex environment. The proliferation of sensor application has increased the need of security in sensor network. At the beginning WSN were not built keeping the security in mind because sensor networks may interact with very sensitive data and operate in hostile unattended environments. It is imperative that at the beginning of the system design, this security concern should be addressed.

In this paper we present the intent to investigate the security related issues and challenges in wireless sensor network. To provide security and privacy to small sensor nodes in terms of computation, communication, memory, storage and energy supply. The security methods for existing networks which include mobile ad-hoc network are not well suitable for wireless sensor networks because of the resource limitations of sensor nodes.

Keywords- DOS; Sybil Attack; black hole attack;, hello flood attack; wormhole attack; LEAP; CSMA/CA.

I. INTRODUCTION

Wireless Sensor Networks have emerged as a dominant technology in the current decade. Diversified application areas of Wireless Sensor Networks indicate the bright future of this new paradigm. The deployment of small, inexpensive, low-power, distributed devices, which are capable of local processing and wireless communication, has been made a reality owing to the recent technological improvements. One can envision in the future the deployment of large scale sensor networks where hundreds and thousands of small sensor nodes form self-organizing wireless networks. Providing security in sensor networks is not an easy task. Compared to

Conventional desktop computers, severe constraints exist since sensor nodes have limited processing capability, storage, and energy, and wireless links have limited bandwidth. Despite the aforementioned challenges, security is important and even critical for many applications of sensor networks. Traditional security techniques used in traditional networks cannot be applied directly, and new ideas are need. In

this paper, we give some security methods to adapt to wireless sensor networks.

We have identified different challenges in providing security to a WSN deployment. We summarize typical attacks on sensor networks. We give typical assumptions and security objectives of sensor networks. Finally, we conclude this article. Due to page limits, we do not extensively discuss other sensor network security issues, such as broadcast authentication and detection of compromised sensor nodes.

II. CHALLENGES

There is always a conflict between minimization of resource consumption and maximization of security level. A better solution gives a good compromise between the two. In order to design the security solution we need to take care of following resource constraint: limited energy, limited memory, limited computing power, limited bandwidth, limited communication range[1] [6].The security mechanism that can be hosted on a sensor node platform is depends on the capabilities and constraint of sensor node networks. The communication in WSN is through wireless media, mainly radio. This characteristics of WSN makes wire base security scheme impractical for a WSN.

The topology of WSN is always dynamic. The sensor nodes can come and go in arbitrary fashion. Again very

often large number of nodes is expected in sensor network deployments and nature of this deployment is unpredictable. Overall cost of WSN should be as low as possible. Ad-hoc networking topology of WSN facilitates attaches for different types of link attacks ranging from passive eavesdropping to active interfering. Attacks on WSN can come from all directions and target at any node leading to leaking of secret information, interfering messages etc [1].

III. ATTACKS AND THREATS IN WIRELESS SENSOR NETWORK

In wireless sensor network attacks can be broadly classified into two different levels, one is the attacks against the security mechanism and other against the basic mechanism like routing mechanism. Here we point out some of the major attacks in WSN [1] [9].

i. Denial of services (DOS) - DOS is produced by the unintentional failure of nodes. DOS attacks exhaust the resource of the victim node by sending extra unnecessary packets, thus presents the network from accessing services. Several DOS attacks might be performed in wireless sensor network in different layers. The mechanism to present DOS attacks includes strong authentification and identification of traffic [9].

ii. Attacks on information in transit- In WSN the sensors are the main monitors and they monitor the change of specific parameters or values and immediately report to the risk according to the requirement. While sending the report the information in transit may be altered or corrupted or vanished. Any attacks can monitor the traffic flow as WSN is vulnerable to ever dropping. Basically the sensor nodes have short transmission range. An attack with large processing power and large communication range could attacks several sensors at the same time [1].

iii. Sybil attack- In order to accomplish a task, the sensors in a WSN might need to work together in many cases. They accomplish this by distributing the subtasks and redundancy of information. In this situation a node can pretend to be more than one node using the identity of other node. Sybil attack is the attack where one node forges the identity of more than one node. Sybil attack affects the integrity of data security and resource utilization [4].

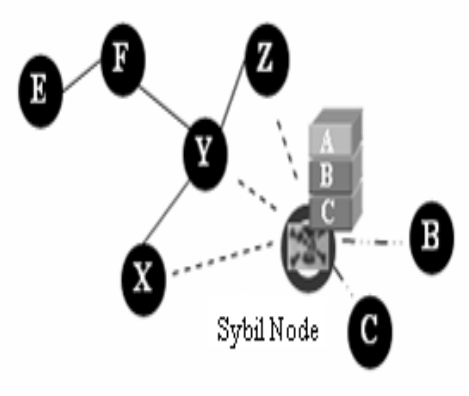

Figure 1. Sybil Attack

iv. Black hole attack- In this attack, a black hole represents a malicious node which attracts all the traffic in the sensor networks. In flooding based protocol the attacks listen to request for router than replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious node convince them base station is only a single hop away from them, thus creates a wormhole [4].

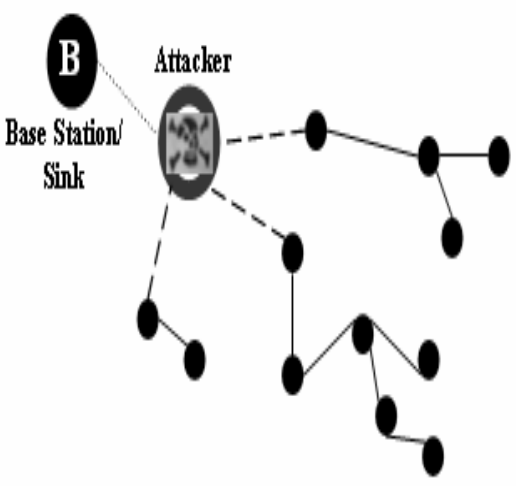

Figure 2. Black hole attack

v. Hello Flood attacks- In this attack the attacks use the hello packets as a weapon to convince the sensor nodes. The attacker does this by sending hello packets to a number of sensor nodes dispersed in a large area within a WSN. Consequently while sending the information to the sink the victim nodes tries to go through the attacks as they know that it is their neighbor and ultimately spoofed by the attacks[1].

vi. Wormhole Attacks- It is very critical attacks in WSN. In this the attacker records the packets (orbit) at one location in the network and tunnels those to another location. Wormhole attacks in a significant thread to the WSN, it

could be performed even at the initial phase when the sensor start to discover the neighboring information [9] [1].

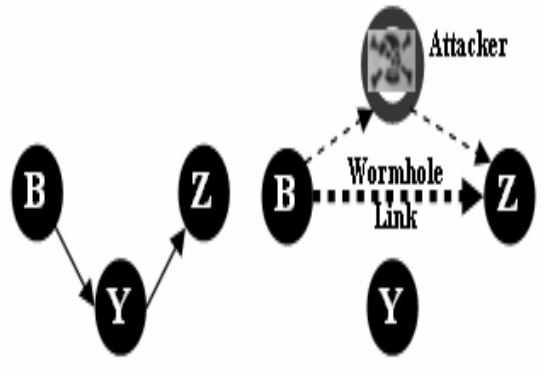

Figure 3. Wormhole attack

IV. APPROACHES TO SOLVE SECURITY THREATS

A.Localized encryption and authentification protocol (leap)

In order to provide confidentiality and authentification in sensor network a multiple keying method is provided by the LEAP. It supports the few types of key established for each sensor nodes. An individual key shared with base station, a pair wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shred by all the nodes in network. Now each of these key is discussed and established in LEAP protocol [10]. Different types of keys are available here:

i. Individual key- Every node has a unique key that it shares pair wise with the base station. In order to communicate between a node and base station this key is used for security. If the node observes any undesired behavior by a neighboring node it may send an alert to the base station. Similarly, this key is used by base station to encrypt any sensitive information, e.g. keying material or special instruction, it sends to an individual node.

ii. Cluster key- This key is shared by a node and all its neighbors. It is used for securing locally broadcast manager. In network processing techniques, in order to save energy in sensor network data aggregation is very important. In LEAP each node process a unique cluster key which is used for securing the message, while the immediate neighbors use the same key for decryption or authentification of its messages.

iii. Pair wise shared key- Each node show a key with its immediate neighbor that key is known as pair wise shared key. In order to guarantee privacy and source authentification, the pair wise keys are used in LEAP. The use of pairwise keys precludes passive participation. For example, a node can use its pairwise keys to secure the distribution of its cluster key to its neighbor.

iv. Group key- this is used by the base station for encryption. The messages that are broadcast to the whole group are encrypted by using this key. An efficient re-keying method is used for updating this key after a compromised node is revoked, since the group key is shared among all the nodes. For e.g. the base station issues mission, sends queries and interacts, node that from the confidentially point of view there is no advantage to separately encrypting a broadcast message using the individual key of each node.

Every node has an individual key that is only shared with base station [8] [10].

Each node has an individual key that is only shared with the base station. This key is generated and pre-loaded into each node prior to its deployment. In this scheme the controller might only keep its master key to save the storage for keeping all the individual keys. The process of establishment of cluster key is very straight forward. In this cluster key establishment phase follows the pairwise key establishment phase. Whenever a node wants to establish a cluster key with all its immediate neighbors then the node first generate a random key then encrypts this key with the pair wise key of each neighbor, and then transmits the encrypted key to each neighbor. The receiving node decrypts the key and stores it in a table when one of the neighbors is revoked; the previous node generates a new cluster key and transmits to the entire remaining neighbor in a same way.

A pairwise shared key is shared only between the node and one of its direct neighbors. A pairwise key establishment is simply done by preloading the sensor nodes with the corresponding keys where the neighborhood relationship are predetermined (e.g. Via physical installation).In the sensor network one key is shared by all the nodes known as group key. When the base station wants to send some confidential instruction to all the nodes in the sensor network one way of doing this is to just distribute a message security to all the nodes using hop by hop translation. The base station encrypts the message with its cluster key and re-broadcast the message. The process is repeated until all the nodes receive the message. In this process each intermediate node is used for encryption and decryption process leads to consumption of huge energy which is a limitation in itself. So to overcome this limitation we use a group key for encrypting a broadcast message. This group key must be changed and distributed to all the remaining nodes in a secure, reliable and timely fashion.

For an example let us consider two key distribution schemes, where there are only two classes of

the heterogeneous sensor nodes (I = 2). The first scheme is a key-pool based key distribution scheme. It is based on the random key distribution and polynomial based key pre-distribution protocol. A pool of randomly generated bivariate polynomials is used to establish pairwise keys between sensor nodes with the consideration of I classes of heterogeneity among the wireless sensor nodes. Compared to the key-pool based scheme, the polynomial-pool based scheme may be more resilient and require less memory storage as well as communication overhead.

For both schemes, we can denote C1 as the class of the less powerful sensor nodes, and denote C2 the class of the more powerful sensor nodes. A C2 node is in the neighborhood of a C1 node, if this node can directly receive a broadcast message from C2 node. It means that C1 node can receive the key (polynomial) pool information of the C2 node without the relay of other sensor nodes. Key management scheme in WSN is shown in the Fig 4.

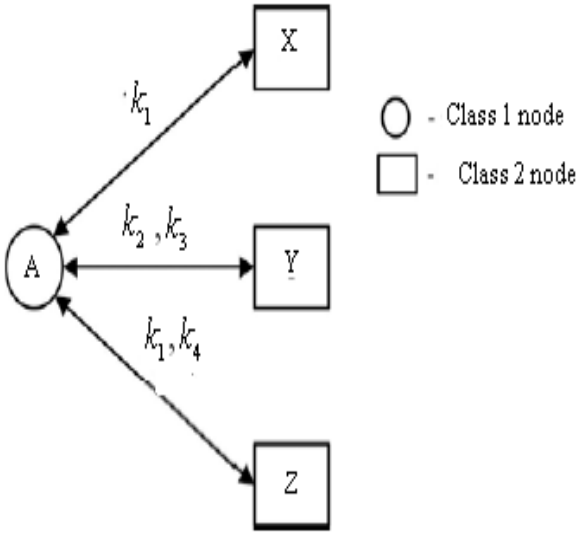

Figure 4. An example of key management scheme in WSN [10].

In this example, nodes X, Y, and Z are the only C2 neighbor nodes of node A. In addition, node A shares key K1 with node X, K2 and K3 with node Y, while K1 and K4 with node Z, respectively. Node A is connected if q 4. In such a case, if node A wants to submit new information to the sink node, it can first randomly selected a key from K1 to K4. Then, it can randomly select a neighbor node that shares the same key with it. In this way, the communication is more resilient, while maintaining the connectivity.

B. CSMA/CA

Carrier sense multiple access with collision avoidance (CSMA/CA) is used in wireless LANs where a transmitting station is unable to determine if a collision occurred while transmitting or not. Collision detection, as is employed in Ethernet, cannot be used for the radio frequency transmissions. The reason is that when a node is transmitting it cannot hear any other node in the system which may be transmitting, since its own signal will drown out other signals arriving at the node. A station will ultimately know when a collision has taken place by reception of negative acknowledgment or by timeout mechanisms [2] [11].

An ad hoc network is a collection of communicating nodes that do not have established infrastructure or centralized administration.CSMA/CA protocol is useful in ad hoc networks where access to the network is decentralized since each station coordinates its own decisions for accessing the medium. There is no central access point to coordinate activities of all station. Thus ad hoc networks are simpler to implement and to modify. The price for this simplicity is that ad hoc networks are prone to collisions.

The main drawback of CSMA protocol comes from the slow collision resolution as the number of active Stations increases. A station will be in one of the following three states at each contention period:

- A successful packet transmission state
- A collision state
- A deferring state

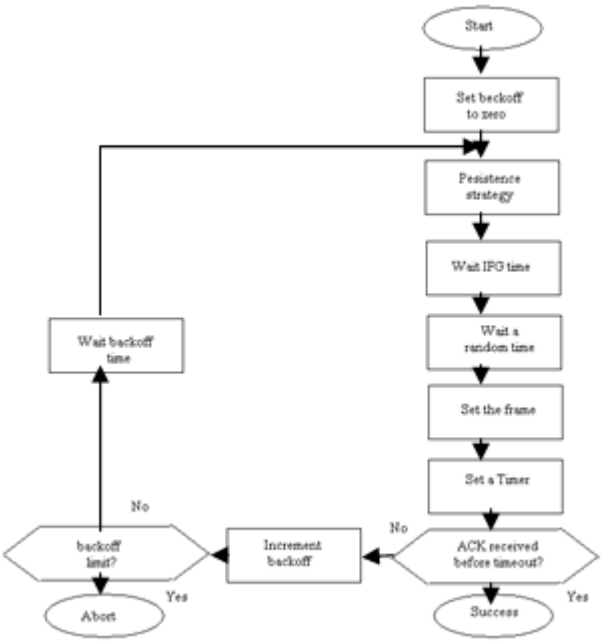

Figure 5. CSMA/CA Procedure [12]

In CSMA/CA, there is no change in the contention window size for the deferring stations. In CSMA/CA the stations wait for the random period of time chosen by the backoff algorithm. It must not consider the system state into account during the backoff period. As a result even when no station is transmitting, the channel passes unutilized and the deferring stations are just waiting. This

causes the wastage of network bandwidth that could be utilized to improve the network performance.

V. PROPOSED SOLUTION

In the possible solution, we consider the CSMA/CA as the MAC protocol and modify the existing protocol by enabling it to adapt according to state of the network, since the existing CSMA/CA protocol does not consider the wastage of bandwidth due to unutilized periods of the channel. So the proposed protocol takes appropriate action whenever unutilized periods detected. In the modified protocol, we changed the contention window size of the deferring stations and regenerate the backoff timers for all potential transmitting stations to actively avoid "future" potential collisions, and take advantage of unutilized slots. In this way, we can resolve possible packet collisions quickly and improve the bandwidth utilization of the network [11] [12].

VI. CONCLUSION

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. Even if holistic security could be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming days.

ACKNOWLEDGMENTS

The authors would thanks the reviewers for their help in improving the document.

REFRENCES

[1] Hiren Kumar Dev Sharma, Ajit Kumar, Sikkim Manipal Institute of Technology 'security threats in wireless sensor networks' IEEE 2006.

[2] Piyush K. Shukla, S. Silakari. Sarita S. Bhadoria, RGVP Bhopal India 'Network security scheme for wireless sensor network using efficient CSMA MAC layer protocol', sixth international conference on Information Technology, 2009.

[3] Xiuli Ren, Norman University, Siping, China, 'Security methods for Wireless Sensor networks', International Conference on Mechatronics and Automation, June 25-28, 2006.

[4] Xiao Jiango Du, North Dakota State University 'Security in Wireless Sensor Network', IEEE August,2008 .

[5] Al Sakhib Khan Pathan, Hyung-woohee, Cheeng Seon Hong, Department of Computer Engineering, Kyung Hee University, Korea'Security in Wireless Sensor Networks: Issues & Challenges', ICACT, Feb 20-22, 2006.

[6] Shuai Xang, Jie Liu, ChuxiaoFan,Xioying Zhang, Junwei Zou, School of Electronics engineering, Beijing University of port & telecommunication, Beijing, China 'A New Design of Security in Wireless ensor Network using Efficient Key Management Scheme.', IEEE 2010.

[7] Jungi Zhang & Vijay Vardhrajan , Department of Computer, Macquire University, Sydney Australia, 'A New Security scheme for wireless sensor network.', IEEE 2008.

[8] Xilin Wang and Mooshang qin, Tiyuan University of Technology, China,'Swcurity For Wireless Sensor Networks.', International Conference on Control , Automation and System, 2010.

[9] Md. Aniur Rehmam & Mitu Kumar Debnath, Dept. of Computer Science and Engineering, Shah Jalal University , Bangladesh. 'Energy Efficient Dta Security System for Wireless Sensor Network.', sixth Intenational conference on Computer and information Technology, 2008.

[10] Ali Nur Mohammad Noman, United International University, Dhanmondi, Dhaka, Bangladesh,'A Generic Framework for Defining Security Environment of Wireless sensor Networks.', 5th interbational conference on Electrical & Computer Engineering ', 20-22 December 2008.

[11] Analysis of Computer and Communication Networks. Fayez Gebali, Springer Publications.

[12] Data Communication And Networking, Behrouz A. Frouzan, Mc Graw Hill Higher Education Publications.

AUTHORS PROFILE

Harmandeep singh received his Bachelor of Engineering B.E and pursuing Master of Technology M.Tech from Guru Nanak Dev Engineering College, Ludhiana ,India.

Garima Malik received her Bachelor of Engineering B.E and Completed Master of Technology M.Tech from Punjabi University Patiala, India. Presently she is working as a Assistant Lecturer in Rayat Bahra Inst. of Eng. and Nanotechnology, Hoshiarpur , India.