ADVANCED NETWORK SECURITY SYSTEM FOR SETUP STAGE OF LEACH PROTOCOL

[1]Rajesh C. Ramannavar, [2]Suma K.V
[1]Student, [2]Assistant Professor
M S Ramaiah Institute of Technology,Bengaluru,India
Email: [1]raaj.rc586@gmail.com, [2]sumakv@msrit.edu

Abstract: WSN is an emerging technology and has found its applications in many areas such as Military applications, defense applications, smart homes, surveillance applications and many more. The major challenge faced in WSN is security. Most of the WSN applications are developed using hierarchical routing protocols for routing the data to the root node. In Leach protocol non-cluster head nodes make decision to join to the cluster head based on the Received signal strength (RSS) of the HELLO packets received from the cluster nodes. This would make it vulnerable to HELLO Flood attack. An adversary laptop-class node will try to send the HELLO packet node with the higher transmission power, so that it tries to convince more sensor nodes in the network that it is their neighbour. In this paper, method is proposed to detect and prevent HELLO Flood attack in the Wireless sensor network. In the proposed scheme, the location of the sensor node, received signal strength of the message signal is considered for detection of HELLO Flood attack. The original key ring and common keys are loaded onto the sensor nodes. The sensor nodes will form secure link with other sensor nodes only if they both have a set of common keys between them else the secure link will not be formed.

Keywords: Wireless Sensor Networks (WSN), RSS Based, Location-dependent key (LDK), Leach Protocol, HELLO Flood Attack.

1. INTRODUCTION

Many sensors nodes are available in the market which has sufficient computing, transmission or receiving powers. Hence more number of sensors can be deployed in a network for any application. The sensor nodes in the network have limited power which must be utilized very efficiently in order to increase the life of the sensor node. No doubt an efficient circuitry is required in all the sensor nodes for ensuring the proper usage of energy, but the routing protocol plays a very important role in energy consumption, bandwidth consumption and security.

In order to overcome these constraints direct transmission approach was proposed. In direct transmission, a sensor node senses the data when available and transmits the data directly to the base station. In this method no doubt data security is achieved, but have to compromise on the power on every sensor nodes as its lifetime would decrease due to the excess consumption of energy by these sensor nodes if the base station is very far. Hence the sensor nodes which are far from the base station would die early than the sensor nodes which lie closer to the base station making some region in the network sensor free and therefore no sensing in those regions.

The approach introduced above produces a problem of energy consumption. To overcome this, data is transmitted to the base station using the multi-hop transmissions. This also has the same problem as compared with the direct transmission [16]. The only difference with the minimum transmission energy is that the far away nodes remain longer as compared to the sensor nodes which lie close to the base station. This is because the nearer sensor nodes will pass all the traffic received from farther sensor nodes to the base station. However, transmission of bulk data from the sensor node requires much energy. In order to overcome this, the concept of direct diffusion was introduced. According to this mechanism, all the sensor nodes in the network will have two hop communications. It is not much energy efficient for wireless sensor network but it provides way for hierarchical clustering protocols. Concept of clustering was found to be energy efficient for wireless sensor networks. If a sensor node network is deployed randomly then the nodes forms the clusters and then a cluster head is formed in each cluster. The sensor nodes transmits the data to the cluster head and it is the work of the cluster head to aggregate all the data received from the sensor nodes and then transmit to the base station. As a result, bandwidth consumption and energy consumption is optimized in the network. They also state that regardless of aggregated data being transmitted from the cluster head to the base station, if the data is transmitted through multiple hops i.e. from one cluster head to the other and to the base station, then the network lifetime would be enhanced further. Today many protocols have been built based on clustering concept each having different attributes and enhancements in the cluster head selection algorithm. Clustered sensor networks are used so that the system delay can be decreased, energy can be saved while performing the aggregation of data and increase throughput of the system.

Wireless sensor networks have found its application in many areas and usually they are used in an open environment. As the sensor nodes in the network are deployed with low energy constraints, these networks are more prone towards different attacks such as Hello Flood attack, wormhole attack, sinkhole attack, Sybil attack, etc. Many protocols that are available make use of the cryptographic and non-cryptographic based approaches in order to use the energy efficiently which is available in each sensor node in the network and along with that to provide security from different attacks such as Hello Flood attack, wormhole attack, sinkhole attack, etc. Among the different attacks Hello flood attack is the most important attack which targets mostly the cluster based protocols such as Leach protocol, AODV protocol, etc. There are many protocols that have been proposed to provide security and optimize the energy in the sensor network. In the cryptographic methods a cipher key is generated by encrypting the key and using this key authentication is performed for the sensor nodes in the network. Many approaches have been proposed which make use of the cipher key. In non-cryptographic method, some parameters of the signal are considered into account in order to decide whether the sensor node is a secure node or it is malicious node. The approaches that are based on the cryptographic methods are suitable for static networks and they have storage overheads, scalability issues, etc. Whereas the other approaches such as received signal strength based detection is not associated with any cryptography primitives, are efficient with respect to the memory storage and with scalability measures. Even though the above method suffers from the certain issues such as the cluster head distinguish the normal sensor node and the adversary node based on the received signal strength of the message. Since RSS is inversely proportional to the distance, if any of the adversary nodes transmits the data from far distance compared to the cluster head then that node will be falsely detected as a friend node. To overcome this situation, the HELLO message receiving node will send the test packet to the HELLO sending node. If the response arrives within the specified time interval then the sender

node is considered as the friend node else it is classified as a stranger node. This would lead to lot of communication overhead in the network as the number of packets that are transmitted in the network would increase. This is because the adversary tries to transmit signal with high energy so that it would convince more sensor nodes in the network that it is a friend node.

2. RELATED WORKS

Most of the approaches that are available make use of the symmetric key approach [14]. In these approaches the nodes will be sharing the keys prior to the communication phase. Symmetric keys are loaded onto each sensor nodes before deployment. These keys are used while forming the secure links between the neighboring sensor nodes during the communication phase of the network.

Many solutions are available regarding the pre-deployed keys in the sensor nodes and also include the approaches where they make use of global key shared among the sensor nodes in the network [15]. There are approaches in which the sensor nodes will be sharing the unique keys with the base station [13] and also some approaches where each sensor nodes will be deployed with some random set of keys [7, 15, 16, 17, 18, 12].

The advantage of using global key is that it will reduce the storage space in the each sensor nodes and also the search time. But it has disadvantage with respect to the security point of view, if any of the sensor node gets compromised then the whole network is compromised. In order to avoid this problem pair wise secret key sharing can be used. This will avoid complete compromise of the network. This scheme will be having perfect resilience because in this scheme if any of the nodes gets compromised then it does not affect the security of the communication link formed with the non compromising node. But the disadvantage associated with this approach is the more storage space required for the keys in the sensor nodes. Also since each sensor nodes will be deployed with many keys, most of these keys may not be used while forming the secure link with the sensor nodes as the sensor nodes will be forming the secure links only with their neighbors. Further the addition of the sensor nodes will be difficult as it involves each of the deployed sensor nodes to be re-keyed.

There is a bit variation to the pair wise key approach where in to have a special node in the network in which all the sensor nodes will share the pair wise key [13]. With the help of this special node the secure links are formed and the communication between the sensor nodes will occur. The disadvantage associated with this approach is the special node vulnerable to attacks and if attacked the entire network is compromised and hence the entire network will become insecure. Also during the communication phase all the sensor nodes have to communicate with the special node this would create a lot of traffic on the nodes near to the special node and hence it would affect the network lifetime.

Now let us consider the approaches where the sensor nodes are deployed with the random set of keys. These approaches are normally known as probabilistic keying approaches. In this approach a large pool of keys are loaded in the sensor nodes prior to the deployment of the sensor nodes. The keys are chosen from the key pool randomly in order to form a secure link between the neighboring sensor nodes. The secure links are formed only if the sensor nodes share some common set of keys among them. There are possibilities that the neighboring nodes may not have common keys at all due to the random distribution of keys in each sensor nodes. Hence there will not be any secure link formed between these nodes. In [16] there is another approach which acts as an enhancement to the probabilistic key sharing approach (Basic Scheme). In this approach if the sensor nodes have to form a secure link with the neighboring nodes then they should have at least some number of common shared keys, else the link would not be possible with these neighboring nodes. Through this approach the resilience of the network is improved. There is a threshold set up for the number of common keys between the neighboring sensor nodes to form a secure link

and if this threshold is increased then the attacking of the sensor nodes will become very difficult by the attacker in order to break the link between two non compromised sensor nodes. On the other hand if the size of the key pool in the neighboring sensor nodes is reduced then there would be some probability of forming the secure link with these neighboring sensor nodes. However in this case if any sensor node gets compromised then the attacking node will have knowledge about the keys in the compromised nodes, since the number of keys size is less only some neighboring nodes may get compromised. This implies that the adversary will have higher percentage of control over the keys in the compromised sensor nodes but less number of sensor nodes. Hence, it would result in the node compromise containment to less number of sensor nodes. The network will be more vulnerable when the large number of the sensor nodes is compromised.

Many probabilistic schemes have been proposed. Most of the schemes that are developed do not make use of the deployed sensor nodes information. There can be significant improvement in the performance of the various schemes if this information is considered. This is due to the sensor nodes which are nearer will have more common keys where as the sensor nodes which are relatively far will have no common key at all [18]. The assumption of the authors is that the information concerning the deployment of the sensor nodes is known. By using this information it can be ensured that the sensor nodes which are close to each other will share some common keys where as sensor nodes which are far from each other will not share the keys.

Another approach which does not require any information of the location co-ordinates of the sensor nodes after node deployment is proposed [11]. However, this approach requires the knowledge of group of sensor nodes that has to be deployed in a given area. Here the expectation is the group of sensor nodes will be placed in the same region. Hence, sensor nodes will be loaded with common keys before node deployment.

Some key management approaches make use of the post deployment knowledge of the sensor nodes [10]. Here the keys are mapped with respect to their locations. Each sensor node will be loaded randomly with excess number of keys. After node deployment each sensor node will determine its location and then it prioritizes the keys loaded on the sensor nodes. The priority of the keys is based on the distance between the sensor nodes and the location of the node through which keys are loaded to the sensor nodes. The keys with lower priority are then discarded where as the keys with higher priority will be used to form secure communication link between the neighboring nodes as in case of other schemes. Hence, this would reduce the storage space in the sensor nodes that could be used for other tasks.

3. SYSTEM MODEL

A number of sensor nodes are deployed in the indoor or outdoor environments. There are anchor nodes in the network along with the sensor nodes in the same region. The sensor nodes and anchor nodes transmit power at different energy levels. The anchor node is assumed to transmit at five different power levels. The sensor nodes are arranged in for of clusters and every cluster has a cluster head. The anchor nodes will be transmitting with the higher power than the sensor nodes. The anchor nodes are placed during the node setup stage each anchor node will transmit the power at a higher level compared to that of the other sensor nodes. These anchor nodes are placed in such a manner that every sensor node in the network is associated with at least one anchor node. The anchor nodes transmit in different power levels. Every anchor node in the network are assumed to have same values for power level number and power associated with them. Attacking nodes are considered and they are placed outside the area where the sensor nodes are deployed. These attacking nodes are assumed to have high capabilities. They transmit power at higher energy levels, they can also eavesdrop on to a

communication link once the sensor nodes are compromised.

4. PROBLEM FORMULATION

To overcome the communication overhead due to packets in the network a new approach is specified to the existing received signal strength (RSS) based approach, which is based on the location-dependent key management scheme [1]. Here the non-CH node compares the received signal strength with a threshold value and if it lies within the threshold value then it is considered as a friend node. Now, if the non-CH sensor node wrongly classifies the adversary node as a friend node then based on the distance calculation and if the distance between the two nodes lies within the threshold value then the link is formed. Further if the adversary sends its wrong co-ordinate location then it may also be falsely considered as a friend node. This can be detected by sending Hello packet. If the Hello packet arrives within the certain time threshold then that node is considered to be as a friend node. After the sensor nodes have joined the respective cluster head then the communication between the sensor node and the cluster head takes place After all these operations now let us consider if any of the nodes in the network are compromised then they remain undetected in the network for the complete round.

To overcome this problem location-dependent key management scheme is used at the node deployment stage where every node in the network are pre-loaded with some certain number of random keys [2]. These keys are not available to the adversary node. And based on these random keys derived keys are generated in all the sensor nodes. If the sensor nodes has to communicate with each other then there has to be minimum number of common keys between them. If the number of keys is less than the threshold value then the secure link will not be formed between these two sensor nodes. after the RSS , distance threshold and the test packet approach if the adversary node is still present in the network and treated as a friend node then for this adversary node to communicate with other sensor nodes in the network it should have the common derived keys with it. Since the adversary node will not be having access to any of the keys nor will it have any common keys, the adversary node can be detected and prevented in this step.

5. LOCATION-DEPENDENT KEY MANAGEMENT SCHEME (LDK)

We consider a network which has resource constrained static sensor nodes. These sensor nodes will communicate with each other only through secure links. An assumption is made concerning the sensor node that it can be added at any time to the network.

We make assumption for the threat model that we consider in this scheme that the adversaries will be having very strong capabilities. The adversaries will have access to all the keys in the sensor nodes which are compromised. An adversary also has the capabilities to eavesdrop on the each sensor node transmission in the network. If any of the sensor nodes gets compromised, then the eavesdropping on the links having encrypted communication that is dependent on the particular compromised sensor node will be successful. The only assumption made is adversaries will not compromise the sensor for an initial small interval of time after the sensor nodes are deployed in the network. And after this small initial interval time the adversaries can introduce an attack and compromise any sensor node in the network.

Given the scenario, one approach is to load the common key on each sensor node in the network before node deployment. After node deployment is done each sensor uses this common key in order to generate the different derived keys compared to each of the neighbouring sensor nodes. After obtaining derived keys on each sensor nodes the common key on each sensor nodes is deleted so that to prevent the adversary from accessing the common key on the sensor node after the initial small time interval of node deployment. Therefore, each sensor node will have different keys and using these keys secure link is formed between neighboring sensor

nodes. Furthermore, if any sensor node is compromised then the links corresponding only to those particular nodes are affected. The above scenario is under the assumption that the sensor nodes are not attacked by the adversary nodes for an initial small interval of time after the sensor node deployment. The problem associated with this approach is that all the sensor nodes have to be deployed at the same time as the common key will be destroyed after the sensor node deployment else the sensor node will not communicate with other nodes that have been added after sometime.

We now address the above problem by using an approach called location dependent keying (LDK) scheme that addresses the shortcoming of the above scheme. Here an extra assumption is made that some or all of the sensor nodes will be transmitting the power at different levels. Different power level indicates the sensor nodes will be transmitting to different ranges.

In LDK, we make use of some special nodes known as the anchor nodes. With respect to the capabilities these anchor nodes are similar to that of the sensor nodes. The main difference between them is that the anchor node has the capability of transmitting the message at different power levels. These anchor nodes are tamper proof. Therefore the numbers of anchor nodes that have to be deployed in the network have to be less as it would lead to cost of the key management.

The anchor nodes can also be placed in other regions also such that the sensor nodes can be able to find out their locations securely. It should be noted that the anchor nodes are not required to be deployed physically in the network. Some sensor nodes can be made to function as an anchor node.

Consider a network having Ns number of sensor nodes and Na number of anchor nodes in the network. Sensor nodes will have three phases in their lifetime

- pre-deployment phase
- initialization phase
- communication phase

In the pre-deployment phase each sensor node in the network is loaded with random set of keys and also with a common key. The anchor nodes in the network are loaded only with the common keys and not with the random set of key rings. After this initialization phase occurs where the anchor node will transmit the message in different power levels and the sensor nodes receiving these power levels will generate their own derived keys using their common keys. Once the derived keys are generated the common keys and the original random set of keys are deleted. But the anchor node common key is not deleted. In communication phase, the secure links are formed between two sensor nodes based on the number of common keys between these two nodes. if the number of common keys between two nodes is equal or greater than the threshold value then the secure link is formed between the two sensor nodes.

6. SIMULATION

A. Simulation Parameters

The proposed work is explained in a sequential manner. First, node set-up has to be done in a given area. The sensor nodes are placed randomly in a 100×100 sq unit. The base station is placed at the centre of the area. The sensor nodes will have a particular radial distance to which it can transmit the power. The number of nodes considered for simulation is 100 sensor nodes. Each sensor nodes will have initial energy associated with them. They will lose certain amount of energy after every transmission. The energy loss is calculated based on the path loss model in the free space. Each sensor node will be having the equal probability of becoming the cluster head, in this case the probability assumed is 0.1. The antenna gain is assumed to be 1. The possible minimum distance is considered as 0.01 and the received signal strength is calculated for that distance and this would be the maximum power which can be received compared to other distances.

B. Simulation Results

Simulation is carried out in Matlab environment and the following results are

obtained. The attacking node transmits the advertisement message and tries to convince other sensor nodes in the network that it is the friend node. The red line indicates two attacking nodes have compromised one sensor node in the network in figure 6.1. Hence it is a sensor node vulnerable to attack. The attack on this sensor node by two adversary nodes is detected as shown in figure 1. This detection is based on the Received signal strength. The sensor node is attacked by an adversary node indicated by a green line in figure 2. And thus detected using the distance based approach

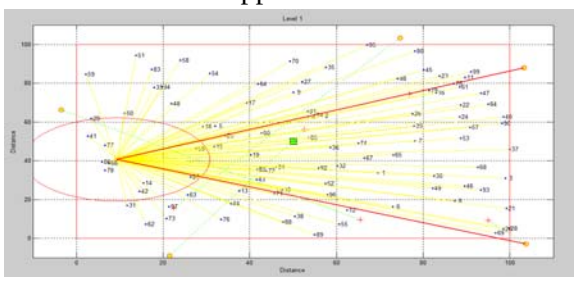


figure 1RSS-based adversary node detection

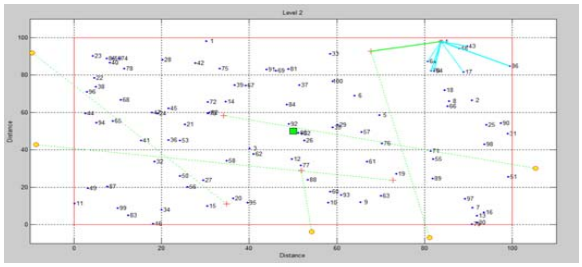


figure 2 Distance-based adversary node detection

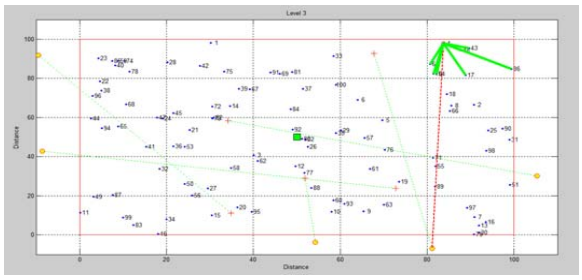
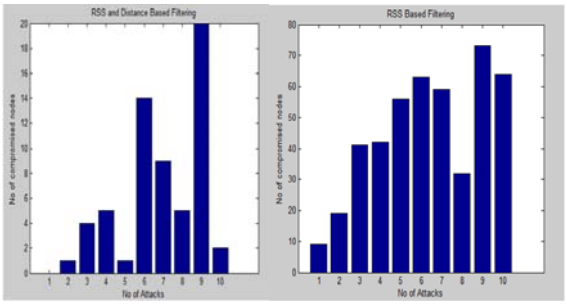


figure 3Test packet based adversary node detection



(a) (b)

Figure 4 (a) No. of attacks vs no. of compromised nodes(RSS based filtering), (b) No. of attacks vs no. of compromised nodes(RSS and Distance based filtering)

If the received signal strength is within the threshold value and if the distance between the two sensor nodes are not within the threshold value then sensor nodes will send test packets to the sensor node which has transmitted this message signal and if the response come within the specified threshold then the sensor node is considered to be as a friend node else it is considered as a compromised node, which is detected as shown in figure 3. Here the number of attacking nodes are varied and then compared with the number of sensor nodes getting affected in the network. As we can observe that the number of compromised nodes is reduced in the distance based and RSS based approach.

7. CONCLUSION

We can conclude that the number of compromised nodes are reduced using RSS and distance based approach. These attacking nodes are prevented in the communication phase as the sensor nodes form secure link only if they have common shared keys else there is no secure link formed between the sensor nodes. Hence, the security for the network is provided.

REFERENCES

[1] Shikha Magotra, Krishan Kumar "Detection of HELLO flood Attack on LEACH Protocol", IEEE International Advanced Computing Conference, 2014, pp. 193-198

[2] Kamal Kumar, Poonam Sharma "Location Dependent Key Management Scheme for Wireless Sensor Network", International Journal of Innovative technology and Exploring

Engineering(IJITEE), Vol. 1, Oct 2012, pp 59-63.

[3] Virendra Pal Singh, Aishwarya S. Anand Ukey, Sweta Jain "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks", International Journal of Computer Applications, Vol. 62, Jan 2013, pp. 1-6

[4] Suraj Sharma, Sanjay Kumar Jena "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks", International Conference on Computer and Computational Sciences (ICCCS), Feb 2011, pp. 146-151.

[5]Reenkamal Kaur Gill, Priya Chawla, Monica Sachdeva, "Study of LEACH Routing Protocol for Wireless Sensor Networks", International Conference on Communication, Computing and Systems(ICCCS), 2014, pp 196-198

[6] Qian Liao, Hao Zhu, "An Energy Balanced Clustering Algorithm Based on Leach Protocol", International Conference on Systems Engineering and Modeling (ICSEM), 2013, pp 72-77

[7] Dahai Du, Huagang Xiong, and Hailiang Wang, "An Effivient Key Management Scheme for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Vol. 2012, Sep 2011.

[8] Haleem Farman, Huma Javed, Muhammad Arshad, Sajid Ullah, "Performance Analysis of High-Resolution Robust Localization and Secure Range Independent Localization in Wireless Sensor Networks", World Applied Sciences Journal, 2012, pp 709-714

[9] Rasheed A, Mahapatra R, "An Efficient Key Distribution scheme for Establishing Pairwise keys with a Mobile Sink in Distributed Sensor Networks", International Performance, Computing and Communications Conference (IPCCC), Dec 2008, pp264-270.

[10] Ashok Kumar Das, "A Key Establishment Scheme for Mobile Wireless Sensor Networks using Post-Deployment Knowledge", International Journal of Computer Networks and Communications (IJCNC), Vol. 3, July 2011, pp 57-70.

[11] Samiran Bag, Bimal Roy, "A new key predistribution scheme for general and grid-group deployment of wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, 2013.

[12] Donggang Liu, Peng Ning, "Establishing Pairwise keys in Distributed Sensor Networks", Conference on Computer and Communications Security (CCS), Oct 2003.

[13] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J.D.Tygar, "SPINS: Security Protocols for Sensor Networks", Mobile Computing and Networking, 2001

[14] Lidong Zhou, Zygmunt J.Haas, "Securing Ad Hoc Networks", IEEE network, special issue on network security, Dec 1999.

[15] Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge", IEEE INFOCOM, Mar 2004, pp 586-597.

[16] Haowen Chan, Adrian Perrig, Dawn Song, "Random Key Predistribution Schemes for Sensor Networks"

[17] Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, "A Pairwise key pre-distribution Scheme for Wireless Sensor Networks", Conference on Computer and Communications Security (CCS), Oct 2003.

[18] Mu Kun, Li Li, " An Efficient Pairwise Key Predistribution Scheme for Wireless Sensor Networks", Journal Of Networks, Vol. 9, Feb 2014.

[19] Chris Karlof, David Wagner, "secure routing in wireless sensor networks: attacks and countermeasures", Elsevier Ad Hoc Networks 1, 2003, pp 293-315.

[20] A Hamid, S Hong, "Defense Against Laptop Class Attacker in Wireless Sensor Network", International Conference on Advanced Communications Technology (ICACT), Vol. 1, Feb 2006, pp 314-318.

[21] Dr. Moh. Osama K., "Hello Flood Counter Measure for Wireless Sensor Network", International