ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Dynamic Key Management System for improving security in Three-Tier environment

P.Kabil dev, II - ME (CSE) [1], O.M. Soundara Rajan[2]

Department of Computer Science and Engineering, Kathir College of Engineering, Coimbatore, Tamilnadu, India[1, 2]

ABSTRACT: Providing security in network field is not a easy thing in each and every network. For wireless sensor network the attackers easily apply their basic probabilistic and q-composite key pre-distribution scheme they compromise the network with the use compromising small fraction of nodes. After that introducing new concept of three-tier security scheme with mobile sinks. But this is not enough against the attacker's harmful mobile sink replication attack. Now we introduce traditional scheme namely Dynamic key management for managing keys against attackers from cluster in a mobile environment. With a new scheme of Duplicated data sending through compromised nodes helps to save the data's against a attackers. They won't get any original data's from this environment. So this concept is providing a network security and also increasing the network lifetime.

KEYWORDS: Dynamic key Management, Attackers, Network Security, Network Lifetime, Three-Tier Security Scheme.

I. INTRODUCTION

Sensors are sophisticated devices that are frequently used to detect and respond to electrical or optical signals. A Sensor converts the physical parameter into a signal which can be measured electrically. Sensors are divided into two bigger parts namely wired and wireless. Wired sensor is a wired communication to send the data using wires. To overcome this, Wireless sensors are introduced. Using wireless sensor we can send the data without wires. An Wireless Sensor Networks are the autonomous sensor, used to monitor the physical or environmental conditions like temperature, pressure, sound etc. The monitored data's are passed through the main location. In earlier Sensor's are used in important fields only, like military, hospitals etc. But now days the technology was reached an great milestone, because the sensor's are used in the small industries, Agriculture etc.

Security in sensor field is an challenging factor in every time. Because of this, the attackers and hackers are the peoples, giving problems to network admin. They need to get information from network using their illegal activities. Sensor nodes are transmitting the information over the network. In earlier Pair-wise key establishment and Authentication are the important factors to improving security. But those things are not enough to block the enemies in network. Attackers having more option to theft the information over the network using a Sybil attack[4], sinkhole[7], wormhole attack[3]. But here they handle an different kind of attack namely Mobile sink replication attack[1] to gain control of network. They simply doing basic probabilistic[12] and q-composite pre distribution scheme to done their work. To rectify this problem, develop a new framework namely Three-tier security scheme that permits the authentication between mobile sinks and sensor nodes based on polynomial pool-based key pre-distribution scheme[14]. If a attacker launch an successful mobile sink replication attacks, then they need to get access of sensor nodes. To block this attack introduce the stationary access nodes for authentication. It act as authentication access point to the network.

A mobile sink sends data request message to the sensor nodes using an stationary access nodes as intermediate agent. This message initiates the mobile sink process and which transmit their data to requested mobile sink. And also an security purpose they using two separate key pools namely mobile polynomial pool and static polynomial pool for carrying keys. Mobile polynomial pool will make it highly difficult for attacker to launch their mobile sink replication attack. So the attackers are disturbed to launch their illegal activities. This mobile polynomial pool keys are used mainly for mobile sink authentication and also gain the control of network for data gathering. So the attackers have no

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

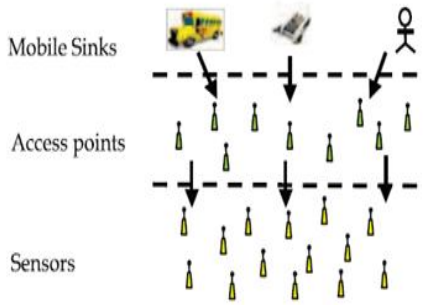
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

way to compromise the nodes in the network. But the attacker followed an different attack to gather data namely Stationary Access Node Replication Attack (SANRA)[1]. Static polynomial pool is located on the stationary access node. So they get the stationary access node as well as the gain control of static polynomial pool and gathering all transmitting data's. An analytical result explains to avoid this attack using an one-way hash chains algorithm[20]. But it may be not enough to control these kind of attack, so introducing an concept of Dynamic Key Management(DKM).



Dynamic key management is an process of managing the keys and also providing the keys to an authenticated nodes only. A cluster has an group of nodes and each and every group has an name like Group A, Group B... Each group has an only one head namely cluster head. The cluster head only having all of the group node keys and provide the keys only the transmitting time. Otherwise the cluster head won't provide any keys to any group, so the nodes in a group having none of the keys. Initially an attacker coming near to the cluster means, the cluster head intimates to all the group about the attacker, so the nodes in a group ready to face an attack. The attackers need to compromise the node to get the data from the network, so they initiate their activity to get data. If an attacker compromised the node, then they easily get the data, so the data's are keep in safe. But the blocking attacker in a wireless sensor field is an seriously bigger problem. So the attacker compromise the node little bit hard. Here introduce a new technique to providing an different kind of duplicated data to sensor node. Initially sending an two kinds of data namely Duplicated data and Original data. If the attacker get access of any node, then they receive the data and read or copy of the data, so the node act as an suspicious node. Then Easily finds that node is an suspicious or attacked node by the attacker. Sending nearest node to the suspicious node to an duplicated data's and the attacker only get the duplicated data's. They won't get any original data's and original data's are send through the destination using the Shortest Path searching algorithm with nearest node. Hereafter the original data's are travel safely in the network without any suspicious attacks. The attackers get access of stationary access node then get ready to get the data's and also ready to launch SANRA [1]. But we finds which node is an suspicious node based on that nodes illegal activity. Provide only the duplicated to the suspicious node, so the attackers think get the data's and those data's are the original. But the original data's are sent through the base station using nearest nodes and shortest path finding algorithm. An attacker finally knows the data's are the duplicated data's. There is no way to repeatedly access the node and data because at the transmitting time only the key will provided for nodes by the cluster head. So an attacker confused to get the data and also confused to get access of stationary access nodes.

II. RELATED WORK

The key management problem is an bigger issue in sensor field. Each and every sensor nodes are needed to transmit the node, then only the data's are reached to base station, so each and every sensor node within a group need an keys to transmit the data. While attacker entered and also get the full access of sensor node, and ready to hack data, but they need to wait. Because the node are none of the keys at the time, transmitting time only the nodes get access of keys from the cluster head. A cluster having a variety of group in the network and each and every groups are specified using their names. All of the groups are having the number of nodes to transmit the information over the network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

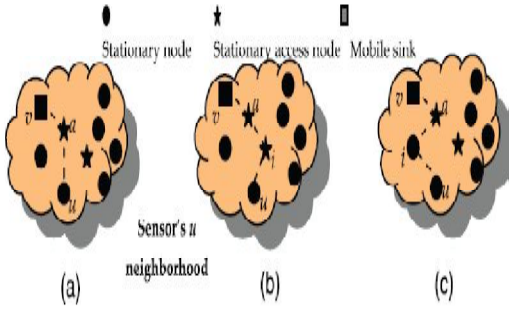
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

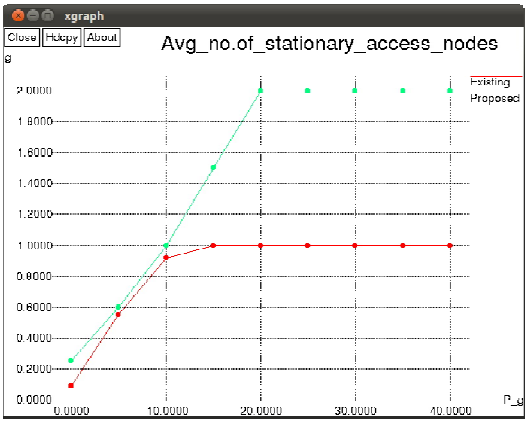
Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The pair-wise key establishment between the sensor nodes are still more difficult to handle. Attackers are not easily handle the sensor nodes, they need to get the full access of node and also they try get the access of cluster. But the cluster get won't allow to compromising the group and the cluster head provide the duplicated data's, if the attacker give any kind of problem to sensor nodes.



Recent advances in wireless technology provide the security of blocking the attackers and also need to eliminate the attackers in the network. But in this paper providing the new technique to handle the attacker using an duplicated data as an backbone and also using dynamic key management in this system to providing the more security of the data's in the wireless sensor network (WSN). So attackers are get confused to finds the original data's. They don't know the original data's are safely send to the base station.



The Key activity of this paper is to avoid the data loss in the network and also providing the safety way to save the network. But the only the pressure work of this paper is the managing the keys, because only the transmitting time only the cluster head to providing the key to group of nodes. So timing of sending key to the nodes are vital work for cluster head. If the cluster head making any late to providing the key to nodes may be the traffic conjunction will occur.

III. DYNAMIC KEY MANAGEMENT

Dynamic key management is an important concept in this proposed scheme. This key management system having lot of keys for distributed to authenticated nodes. Using this key management concept giving more securable transaction of data's in rare network. Which means to save the data's from attackers and send the sensed data's to the authenticated nodes. While attacker try to compromise the node, but they won't does it. Because the nodes don't have any keys at

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

normal time, only the transaction time only the nodes got the key. At normal time the attacker won't get any nodes, so the cluster head also don't have any pressure to do the providing work. While the transmitting time cluster head initialize the work to assigning the keys to all of the nodes and also ready to provide the keys. The nodes are got the keys and also ready to do the transmitting work without compromised by attacker. If an attacker got an key means, they trying to get the data's and also the delaying the network transactions.

If an attacker got the key and they get the data's means, the timing delay was happened due to use the data. Then we easily finds an intruders was absorbs our network, so initialize our safe activities. Which means finds the particular nodes from the cluster, they compromised and make an point of that node. Just don't send any data's to that particular nodes, send the nearest nodes. Send the duplicated data's to compromised node also send original data's to nearest nodes through destination. So no data loss and data theft was happen and also our network also safe.

(i) Security analysis using one-way hash function

A one-way hash function h: a →b is a function with the following properties:

1. The function h takes a message of arbitrary length as the input and produces a message digest of fixed length as the output.
2. The function h is one-way in the sense that given as easy to compute h(a)=b. However given b, it is hard to compute h^{-1} (b) = a.
3. Given a, it is computationally infeasible to find to find $a^{|}$ such that $a^{|}$ a. But h ($a^{|}$) = h (a)

4. It is computationally infeasible to find any pair a, $a^{|}$ such that $a^{|}$ a. but h ($a^{|}$) = h (a).

In the security scheme each sensor node (u) is preloaded with a subset of Ks polynomials randomly chosen from the static pool. In addition to Ks preloaded static polynomials, node u randomly picks a subset of Gs passwords from the password pool. Subsequently for each of the Gs password that has been randomly chosen by node u, its rth hash value is loaded into node u. Each password is blinded with the use of a collision-resistant hash function such as MD5. Due to the collision-resistant property it is computationally infeasible for an attacker to find a value.

To establish an authentication between a sensor node and a stationary access node in the enhanced scheme the two must share a common static polynomial. Also, they need to discover at least a single access node verification for which both the sensor node and the stationary access node have the same password randomly chosen from the password pool. In the access node verification verify the authenticity of a stationary access node, the sensor node performs a single hash operation on the hash value that is sent from the stationary access node. The mobile sink establishing secure links with the sensor nodes from any authentication access point in the network is given by

$$P_{conn} = 1 - \left(1 - p \times \frac{c}{n}\right)^{m}$$

Where n represents the total number of sensor nodes in the network, c is the average number of neighbour nodes and m is the number of stationary access nodes in the network.

(ii) Key Pre distribution Phase in dynamic key management

In proposed scheme an authentication key KCHAuth is a pair of public/private key Kpt/Kst and a certificate CertCHt signed by the base station are pre distributed in each cluster head. The authentication key KCHAuth is used to verify member sensor node identities. KCHAuth is known to all cluster heads and the base station. The public/private key pair Kpt/Kst is used to establish pairwise keys among cluster heads. An authentication key KAuthi and the public key KPBS of the base station are pre distributed in each member sensor node. KPBS is used to verify the certificates of the cluster heads. KAuthi can be calculated by the following hash function:

KAuthi = H (IDi||KCHAuth) (1)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

(iii) Authentication and key seed distribution procedure

With the pre distributed authentication key KAuthi, the sensor node can compute an authentication message auth msgi as follows:

auth msgi = H (IDi||KAuthi) (2)

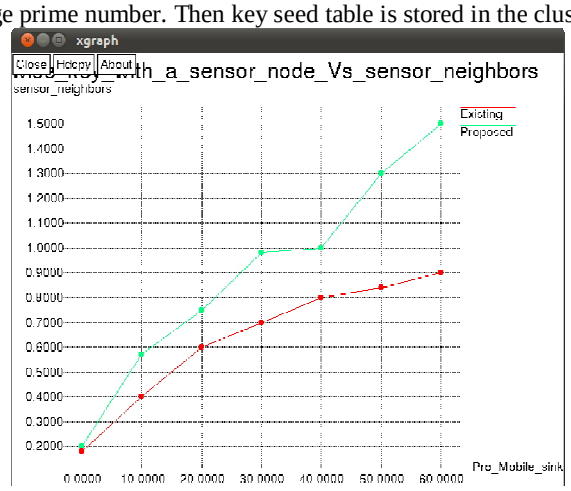
When the cluster head CHt receives the authentication message from Ni, it verifies the member sensor node identity:

auth msg_i= H (IDi||H(IDi||KCHAuth)) (3)

CHt compares auth msg_i with auth msgi. If they are equal, CHt sends a key seed Seedi to node i. Assume there are M sensor nodes in cluster t. The cluster head CHt chooses a large prime number rt and a modulus p. The key seed Seedj is calculated by the following equation:

Seedj = kj p + rt j = 1, 2, . . . , M (4)

The value kj is only known to the cluster head CHt. With the authentication key KCHAuth and the sensor node ID, the cluster head can compute each sensor node authentication key KAuthi by (1) on the fly. The key seed Seedj is encrypted by Ni authentication key. After sensor node Ni receiving the encrypted key seed message, it decrypts this message to get the key seed and then it deletes its authentication key and the base station public key immediately. Otherwise the cluster head drops the JoinReq message. Each member sensor node in this cluster gets its key seed (Seedj) respectively. In order to prevent the key seeds from a brute force attack, the value kj should be a large integer and the value p should be a large prime number. Then key seed table is stored in the cluster head (CHt).



IV. CONCLUSION

In this paper proposal of Dynamic key management and Duplicate data sending for Improve security in three tire environment is very important for save the data's from the third party peoples like intruders. Providing security to network is not an easy thing. But trying to save our network, if we have an biggest idea about network. So choosing the key management issue will briefly explains the saving activities of data's.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

REFERENCES

[1.]I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Surevey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[2]T. Gao, D. Greenspan, M. Welesh, R.R. Juang, and A. Alm, "Vital Signa Monitoring and Patient Tracking over a Wireless Network,"Proc. IEEE 27th Ann. Int'l Conf. Eng. Medicine and Biology Soc. (EMBS), Sept. 2005.

[3]A. Rasheed and R. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Network with Mobile sink", Parallel and Distributed System, vol.23,no.5, May 2012

[4]A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for Heterogeneous Sensor Networks," Proc. Int'l Conf. Wireless Comm. And Mobile Computing Conf. (IWCMC '09), pp.263-268, June 2009.

[5]L. Eschenauer and V. D. Gilgor, A Key-management scheme for distributed sensor networks," Proc. Of the ACM Conference Computer Communication Security (CCS'02), pp.41-47, 2002

[6]Prameels. Bagewadi and Anil Kumar.K "Detection Of Mobile Sink Replica In Wireless Sensor Network And Authenticate It With Key Distribution" (IJERT), ISSN:2278-0181, Vol. 2 Issue 6, June 2013.

[7]B.J. Culpepper and H.C. Tseng , "Sinkhole Intrusion Indicators in DSR MANETs,"Proc. First Int'l Conf. Broadband Networks (Broad-Nets '04), pp.681-688, Oct. 2004.

[8]Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, "Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors," Proc. 13th Int'l Conf. Computer Comm. And Networks (ICCN '04), Oct. 2004.
[9]A. Rasheed and R. Mahapatra, "An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks," Proc. IEEE 27th Int'l Performance Computing and Comm. Conf. (IPCCC '08), pp. 264-270, Dec. 2008.

[10]L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol, 24, no. 11, pp. 770-772, Nov. 1981.