Secure Routing in Cluster based Wireless Sensor Networks using Symmetric Cryptography with Session Keys

Rayala Upendar Rao

Department of Computer science, Vignan University, Guntur -522213, INDIA

ABSTRACT

Wireless sensor network is an emerging technology, uses in many applications like boarder area enemy tracking system, fire alarm system, etc. Sensors are low power devices which possess huge attacks. These low power devices are not suitable for complex cryptographic algorithms. In this paper we implemented symmetric key algorithm with session keys. This concept carry better security compared previous secure routing algorithm in cluster wireless sensor networks. Here the forwarding node will check the both secrete global key and session key. It also checks one more parameter that is loading time of node, ensures more security.

Keywords— Security, Routing, session key, Secrete key, Cluster

1. Introduction

Wireless sensors network playing critical role in each every field. Sensors replacing man power, which can be deployed where human interaction is not possible .For example if we consider boarder area instead of keeping more security force at boundaries for enemy intrusion observation deployed wireless sensor will record the moment enemies and send alert to message to security office or owner (we can call it as Base Station).

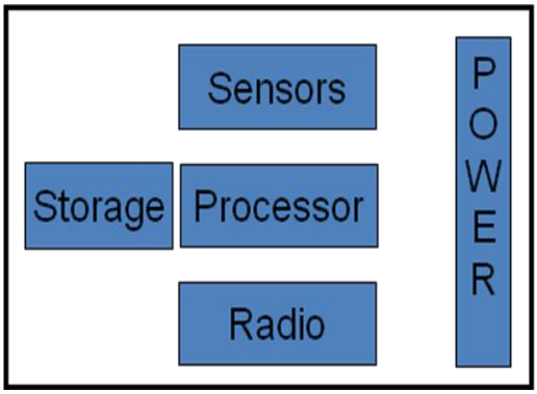

Figure.1. Sensor components

Wireless sensor network posses huge number of attacks like spoofed, altered and replaying; selective forwarding; Sybil; sink hole; worm hole; flooding; acknowledgment[1] , etc. A lot of research work has carried out on sensor network, everybody concentrated for optimizing the performance of sensors according to limited capabilities. Very few researchers consider security as well as routing; they proposed many schemes [2], but no scheme mitigates the all attacks. To overcome these drawbacks we have to concentrate for more efficient secure routing protocol.

Hence there is a necessity to propose new routing scheme secure routing in cluster based wireless sensor network with session keys by symmetric cryptography (SRCWSNS). Proposed session key concept is to change the key after certain time interval. Even though an adversary compromised one node, it will effects only part of the network but not whole. We assumed that cluster topology is suitable for wireless sensor networks why because cluster topology will give a good organization of network nodes, resources and ensures efficient routing.

Proposed scheme easy to understand and takes little amount of memory for storing keys. Overhead is also lesser compare to complex cryptograph based protocols. We implemented this on ns2 simulator, which has given better results compare to existing protocols.

Remaining paper is organised as follows, in section 2, we explored related work (existing work). In section 3 we included comparison of ad-hoc and wireless sensor network. In section 4 we discussed problem statement. In Section 5 we explored about our proposed method. In section 6 we have given comparative experiment results, in last section included conclusion and reference papers.

2. Related Work

A lot research work carried out in wireless sensor networks and lot advancements have taken. Still there is necessity to carry out new technology in wireless sensor network. Cluster routing model more energy efficient model compare to direct or multi-hop routing. Initially we discussed about different proposed schemes on secure routing in cluster based wireless sensor networks, later on we discussed different routing protocols.

Cluster routing model is efficient still there are some issues as well. Wendi Rabiner Heinzelman at al [3] discussed about load balancing concept in cluster routing of low energy aware cluster head routing protocol, he proposed novel idea of CH algorithm for load balancing of cluster head.

Seema Bandyopadhyay and Edward J. Coyle [4] proposed An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks. This technique restricted the advertisement cluster head by k hops thus unnecessary advertisements removed.

Taejoon Park, and Kang G. Shin [5] implemented Secure Routing Based on Distributed Key Sharing in Large-Scale Sensor Networks, it contains two protocols for secure routing a secure geographic forwarding protocol (SGFP) and a temporal-key establishment Protocol (TKEP). It' light weight protocol and mitigates Sybil and selective forwarding attacks.

Peng Ning, An Liu and Wenliang Du [6] introduced Mitigating DoS Attacks against Broadcast Authentication in Wireless Sensor Networks. It provides broadcast authentication based on symmetric cryptography by delayed disclosure of authentication keys. A major limitation of µTESLA and its variations is the Authentication delay. In

other words, a receiver cannot authenticate a broadcast packet immediately after receiving it.

Yun Zhou, Yanchao Zhang, Yuguang Fang [7] proposed Access Control Mechanism in Wireless Sensor Network. It has proposed on Elliptic Curve Cryptography.it provides great security compare to RSA and takes less memory size. But the disadvantage is, for digital signature verification it takes more time, nearly 1.6sec.

Mandicou Ba, Ibrahima Niang, Bamba Gueye [8] presented A Deterministic Key Management Scheme for Securing Cluster-Based Sensors Networks. Here Author introduced DKS-LEACH for secure communication. It ensures low overhead compare with LEACH protocol. But it Management of keys between base station and cluster head, cluster head and its member nodes takes time.

Wang Xiao-Yun, Yang Li-Zhen and Chen Ke-Fei introduced [9] S-LEACH Secure Low Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks. This scheme has given extensive practical scenarios of attacks and analysis of those attacks. Here the disadvantage, Cluster could not change dynamically and it does not provide more nodes, which are nearer to base station to distribute high overhead.

S.NO	Protocol name	Description	Advantages	Disadvantages	Attacks
1	Secure Routing Based on Distributed Key Sharing in Large-Scale Sensor Networks[5]	proposed two protocols for secure routing a secure geographic forwarding protocol (SGFP) and a temporal-key establishment Protocol (TKEP).	It' light weight protocol and mitigates Sybil and selective forwarding attacks.	To implement this we need more equipment like servers for distribution of keys. But this is not possible hostile environment like boarder area security system.	Still it possessed attacks like worm hole; flooding and lap tap class attackers.
2	SNEP & µTESLA[7]	These two protocols are using for DoS attacks and broadcast authentication	It provides broadcast authentication based on symmetric cryptography by delayed disclosure of authentication keys.	A major limitation of µTESLA and its variations is the Authentication delay. In other words, a receiver cannot authenticate a broadcast packet immediately after receiving it.	Still facing DoS and authentication of broadcasting messages.
3	Access control in wireless sensor networks[6]	It is developed on Elliptic Curve Cryptography (ECC).	it provides great security compare to RSA and takes less memory size	For digital signature verification it takes more time, nearly 1.6sec	Cannot mitigate the malicious new in the vicinity of compromised node.
4	A Deterministic Key Management Scheme for Securing Cluster-Based Sensors Networks[13]	Author introduced DKS-LEACH for secure communication.	The secure communication overhead is very low compare with LEACH protocol.	Managing of keys between base station and cluster head, cluster head and its member nodes takes time.	DoS and lap tap class attacks
5	SLEACH Secure Low. Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks[14]	It is an extension to LEACH protocol and uses symmetric efficient one-way hash chains and inexpensive symmetric operations rather than expensive asymmetric cryptography operations.	This scheme has given extensive practical scenarios of attacks and analysis of those attacks.	Cluster could not change dynamically and it does not provide more nodes, which are nearer to base station to distribute high overhead.	Because of symmetric mechanism if node compromised, then whole system is able to compromise by hacker
6	Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks[15]	It has developed on diffie-hellman key algorithm. Author proposed architecture contains three modules pre-node deployment, key dissemination, report forwarding.	It mitigates DoS attacks and false reports injection.	But proposed scheme applicable for only fixed size networks, they are not discussed about new node deployment which creates a bad life time of sensor network.	Wireless sensors have limited capabilities. But takes large memory to save keys and leads to overhead. No attacks possible against this protocol

Table.1. Pros and cons of different routing protocols

3. Comparison of Ad-Hoc And Sensor Network

Sensor network is similar to ad-hoc network but differs in some aspects. In both networks the nodes had capable to move. In both networks uses air as medium to communicate with other neighbouring nodes. Both networks resource constrained, but comparatively mobile ad-hoc network nodes having more capacities in terms of battery life, computing power, transceiver, communication range. In ad-hoc network communication possible for each pair of nodes where as in wireless sensor network the communication categorized into three ways.

A. Many to one communication (nodes to base station)

All sensors sense the environment properties from their surroundings and send that information to the base station (BS) which acts as owner for the network. Here we are considering cluster topology so the information should traverse through the CH. Here the cluster head is able to check the location of the sensor nodes and session key has given by the base station. Likewise the information will reach the BS. Then base station has to verify the identity of neighbour cluster node which sends the data to it, and also it has to verify the session key and time stamp value.

B. One - many communication (base station to all nodes or set of nodes)

This communication will happen among BS and nodes. Whenever the information is needed, the base station will send request to all nodes to know the current status of the surroundings of the environment. For getting information BS is able to broadcast the request or it may multicast the request. Here there is a possibility to come an attacker flood the request as BS, so to remove the drawback CH's have to save the time stamp values assigned by the base station. By using this value any cluster node will verify the base station identity. After verifying the identification, CH forwards the request given by the base station to the nodes which are in its group.

C. Neighbour discover, session key transmission (among the nodes)

This type of communication will occurs when the nodes which require to find out the neighbours. Discovering of nodes is useful after pre-node deployment; the nodes should able to find the neighbour by sending the request with the energy. CH has to send the session keys to its cluster members.

Nodes in sensor network exhibit trust relation among the nodes those that beyond the ad-hoc networks. For sending request or similar information to the base station is, wast of band width and energy of sensor node, to run network in effective way we should use the aggregation, in-networking process and duplicate elimination.

4. Problem Statement

D. Network Assumptions

Typically wireless sensor network refer to heterogeneous consists of tiny devices in hundreds to thousands. Each sensor should have unique identifier or location and load with the bootstrapping time, this time should be equal to all nodes with tolerate value. Sensors are having capable to move from one location to another location, but in many cases sensors having fixed location until their life time expires. Base station should have more capable to store the information like nodes locations, symmetric security key, session keys for cluster heads (CH), time stamp values of CH's, prime field which is defined over elliptic curve and could able to give the interruption to the nodes for new sessions. The nodes should have capacity to forward the data towards the destination. The nodes which are near to base station should have the more capacity to store the different key values and are able to distribute the load equally.

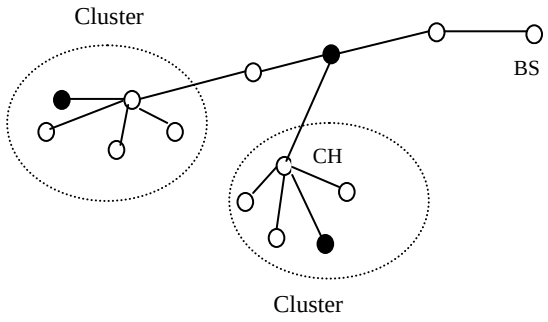

Figure2. Cluster topology

After deploying sensors they form clusters, each cluster contains at least n nodes. In each cluster one node randomly selected as cluster head. To balance energy conservation each node takes turn to act as cluster head. Above Fig. illustrates the organization of sensing nodes in wireless sensor networks. In the figure, CH and BS denote *Cluster- Head* and *Base Station* respectively. Black circles indicate malicious nodes that divert the routing information or steal for their personal use.

E. System Model

Wireless sensor network consist of number of sensor nodes. Each sensor node is able to cover some region with radius r, which is called transmission range of node. Here we consider only bidirectional links assumed among all nodes. Sensor nodes may be deployed in some target field to detect events within field. For example in military may be deployed in hostile environment to detect the movement of enemy forces.

F. Threat Model

Typically sensor nodes deployed in hostile environment so those don't have capacity to resist adversaries. The author assumed that each cluster contains at most t-1 compromised nodes, which are collaborates one other to make the network as vulnerable.

5. Proposed Scheme

Limited capabilities of wireless sensor network are not suitable for complex asymmetric cryptographic algorithms. So we consider this as bottleneck for performance of wireless sensors. To remove this drawback we came with new proposal on security of wireless sensor network with symmetric algorithms.

Even there is lot of work carried out on symmetric cryptography, but the disadvantage is, if any opponent came to know any node key then he has cable to disable the entire network. So to remove this drawback some authors proposed session key establishment with base station (BS), but this concept still having drawbacks. To compensate these problem we introduced the concept session key generation from prime field. Here the prime should be defined in the order of elliptic curve. We assumed that cluster topology will give the best performance over ad-hoc manner and also organisation of nodes in cluster topology is easy. Our proposed scheme SRCWSNS architecture contains three modules. Each module can do specific function; they are pre-node deployment, cluster formation/ cluster head selection and session key establishment.

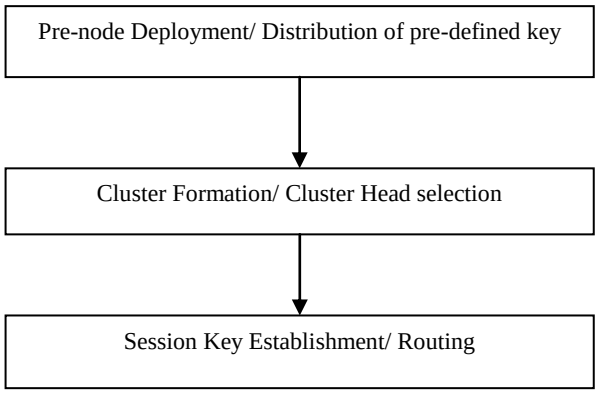

Figure3. Architecture for SRCWSNS

G. Pre-node Deployment/ Distribution Pre-defined key

Initially we need to deploy the nodes manually. Deploying of nodes may be onetime activity or continues process. If it is continuing process, the network life time should extend. Deploying sensors should be continues why because wireless sensor are tiny devices which are having limited power, after some time the energy these devices will be exhaust. So to replace those exhausted sensors or those who got repaired. These wireless devices are deploying in hostile or harsh environment, they should have capable of self managing power.

After deployment of nodes, we should load the sensors with pre-defined symmetric key. For providing encryption we considered blowfish symmetric algorithm, it provides 64-bit block size and a variable key length - from 32 bits to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. While doing key scheduling, it generates large pseudo-random lookup tables by doing several encryptions. It takes fewer bits for key and provides high security. This algorithm is best suitable for wireless devices.

H. Cluster Formation / Cluster Head Selection

After deployment of sensors they should have able to form the clusters. Initiation of Cluster formation will start by any node that sends request to other neighbour nodes by placing its energy level. Then immediate node in that region will replace its energy is greater than previous node otherwise it should forward to its neighbour within region. After passing the request over all nodes in specific region, receive the message the node which has highest energy. Then after it broadcast the status of the node as Cluster Head (CH) and join request to all other nodes. The nodes sent confirmation request those are interested to join, after cluster formation CH has to send the status of node to base station and the base station will save the status and time stamp value for further use and also returns the time stamp value to CH for verification of BS identity, during this transmission we have to use Blowfish symmetric algorithm for mitigating the attackers.

There is possibility of more than one clusters in same region, so one node is able to participate more than one cluster. At this time we should remove the conflict by sending the received signal strength indicator (RSSI), if node receive join request from more than one node it should select high RSSI value node as its cluster. This procedure will repeat until all clusters formed. Here the base station maintains the nodes identity by assigning unique random number in particular confidential series. The cluster head has to change after 3 or 4 sessions. We can choose this factor depends on the situation.

Algorithm for cluster formation and cluster head selection

1. Initially any node could start by placing the energy level of node with request message to its neighbour.
2. The neighbour could check the energy level previous node and replace the value with its energy level value if it has more than previous node.
3. Above procedure repeated until all the nodes covered in particular region and finally the node get the message highest level energy.
4. The node should broadcast the status of as CH node and join request message to all other nodes which are in coverage area.
5. If neighbouring nodes received more than one join request
   I. Check the both RSSI values of CH's and sent confirmation to which is having higher value
   OR
   II. Confirmation message has sent to CH.
6. CH has to send the status information to BS and returns the time stamp value further use to CH.
7. This procedure repeated till all regions covered in network

I. Session Key Establishment/ Routing

Base station will store the elliptic curves, and we should select the prime number in convenient range. Prime filed consist of number of points in range of prime number which are must defined on curve. To crack the key in prime field is very difficult defined over elliptic curve. It provides good security over random number generation.

The base station unicast the session key and time stamp value to cluster head. The cluster head verifies with time stamp value assigned by base station. If the base station has valid time stamp value then it receives the message and broadcast the session key to all its neighbours. Here every session key has particular time out value, so after time out value base station need to request new session key by sending time stamp value assigned by base station at the time of cluster head selection.

Algorithm for session key establishment/routing

1. BS selects the random number from prime field over curve in the range of prime number.
2. BS unicast the information of session key to CH.
3. CH verifies BS with time stamp value assigned by BS previously. (except initial round)
4. CH broadcast the session key to all its neighbours.
5. This procedure repeats for all clusters in the network.
6. After expiring session CH has to send request for new session key.

6. Comparative Results

We compared our proposed SRCWSNS with sec-LEACH protocol. Sec-LEACH is one of the popular protocols used in cluster based wireless sensor networks. Sec-LEACH mitigates all most attacks except sink hole and wormhole attacks. In Sinkhole attack, intruder sends high quality link to the destination even. So the main aim of sinkhole attack is to steal the information. This sinkhole attack will leads another attack that is wormhole attack. This will happen with two nodes, one node takes the incoming traffic another one to transmit the information to out. When the sinkhole intensity is high then we commonly referred as wormhole attack.

Consider the following scenario will give explanation for the mitigation of sinkhole attack. Here node M act as

legitimate node, which compromises the immediate neighbour cluster head node location. The forwarding cluster head checks the identity of M node and checks the symmetric key. Even M got symmetric security key the forwarding cluster head checks loading time of the node or bootstrap time, it ensures more security. These keys are encrypted by using blowfish symmetric algorithm. So to find out these keys are very difficult. It takes more time to crack the keys, in meanwhile the base station will change the session key. So to steal the information from nodes intruder again try to deciphering the content to get the session key.

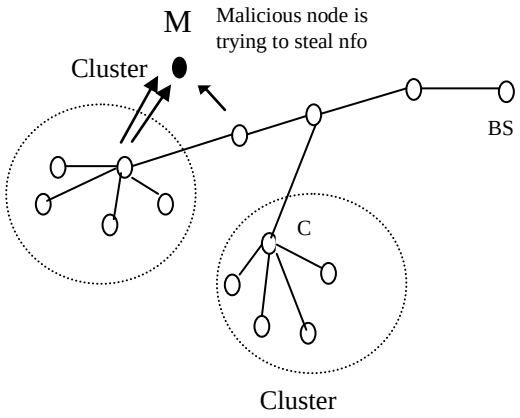

Figure 4.Mitigation of sinkhole attack

Even if the malicious node will compromise one node there is no possibility to compromise other nodes through this one. So the effect of node compromising will restricted to only portion of the networks. Likewise forwarding node will detect the malicious node and also mitigates wormhole attack.

7. CONCLUSION

Wireless sensors are low capable devices that are not suitable for complex asymmetric key algorithms. Because of limited capabilities everyone is trying to optimize the performance of routing. Some of the algorithms based on symmetric cryptograph techniques but they are not mitigating all attacks. By using one attack, intruder is trying do other attacks through this one. For example selective forwarding attack will leads to sinkhole attack and wormhole attack. Because of these factors motivated to introduce new concept of session which are defined in prime field over elliptic curve. So nobody can detect the session key generation and mitigates all most all attacks.

REFERENCES

[1] Hemanta Kumar Kalita and Avijit Kar, "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009.

[2] Chris Karlof David Wagner, "Secure Routing in Wireless Sensor Network: Attacks and CounterMeasures", Ad Hoc Networks 1 (2003) 293–315.

[3] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan," *Energy-Efficient Communication Protocol for Wireless Microsensor Networks",* Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000.

[4] Seema Bandyopadhyay and Edward J. Coyle, " An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Netwroks", IEEE INFOCOM 2003 Twentysecond Annual Joint Conference of the IEEE Computer and Communications Societies IEEE Cat No03CH37428 (2003), 1713-1723.

[5] Taejoon Park and Kang G. Shin, "*Secure Routing Based on Distributed Key Sharing in Large-Scale Sensor Networks*", ACM Transactions on Embedded Computing Systems, Vol. 7, No. 2, Article 20, Publication date: February 2008.

[6] Peng Ning, An Liu,and Wenliang Du, "*Mitigating DoS Attacks against Broadcast Authentication in Wireless Sensor Networks*", ACM Journal Name, Vol. , No. , 20, Pages 1–31.

[7] Yun Zhou, Yanchao Zhang, Yuguang Fang, "*Access control in wireless sensor networks*," Ad Hoc Networks 5 (2007) 3–13.

[8] WANG Xiao-yun , YANG Li-zhen, "SLEACH Secure Low. Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks", WUJNS Wuhan University Journal of Natural Sciences Vol.10 No. 1 2005 127-131.

[9] Mandicou Ba, Ibrahima Niang, Bamba Gueye, "A Deterministic Key Management Scheme for "Securing Cluster-Based Sensors Networks", 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, ISBN: 978-0-7695-4322-2.

[10] Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and countermeasures," Ad Hoc Networks 1 (2003) 293–315.

[11] Pooja Kumari, Mukesh Kumar, Rahul Rishi, "*Study of Security in Wireless Sensor Networks*", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (5) 2010, 347-354.

AUTHORS PROFILE

Mr. Upendar Rao pursuing M.Tech (2009-2011) in the branch of Networks and Internet Engineering in Pondicherry University, India. He received B.Tech degree in Computer Science and Engineering from Kakatiya University, India in 2009. Presently doing research project on Secure Routing in Cluster based Wireless Sensor Networks. His area of interest is computer networks, Network Security and Database Management Systems.