ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Wireless Sensor Network with a Novel Key Distribution for Improved Four-Tier Network Security.

S Poonguzhali*.

Department of ETCE, Sathyabama University, Chennai, Tamil Nadu, India.

ABSTRACT

Wireless sensor network is built of “nodes” from a few to several hundreds or even thousands, where each node is connected to one (or several sensors). So far, more research has focused on making sensor networks for feasible and useful, but not concentrated on security. In order to provide security for the transmitted data between the nodes several layers of security schemes have been involved. Here four tiers security model has been proposed in order to protect the data transferred between sink and other sensor nodes through the access points. The existing key pre-distribution in three tier security which involves static and mobile polynomial where initiating sensor nodes through stationary access nodes so that an attacker can easily identify maximum number of keys to misuse the nodes. Hence by enhancing the existing three tier scheme by adding fourth tier called watcher node in order to evaluate the individual nodes performance and it detects link path. Hence the data will be transferred between the nodes without any change made by an attacker.

Keywords: Improved four tier security, watcher node, sensor nodes, key pre-distribution.

**Corresponding author*

INTRODUCTION

Wireless sensor networks can be defined as a self- configured and infrastructure-less wireless networks. It will monitor the whole set up by passing their data through the network to a sink where the data can be analyzed and verified. A sink and base station acts like an interface between users and networks. It contains several hundreds or thousands of nodes to transmit the data to other nodes in order to reach sink. Hence while the nodes are transmitting data the attacker can modify the data by altering the keys in existing system. Because of that modification of keys data will not be secure[1]. Hence in our idea a fourth tier called watcher node to identify the link path is added. Four tier security system contains four stages:

- Sensors are the first stage of four tier security. Here data will be sent by initiating this process. The information is passed to next stage which is nothing but access point. When the data collected by the access point it will ask for key verification. Then it will be checked and proceed to next stage.

- Access Point. Information collected in access point will proceed to next stage which is watcher node. Here it will ask for key. The key will be generated randomly. Sink will request the messages from sensors. Each node while transmitting, random key will be generated.

- Watcher node. Here link path will be identified before reaching to sink. Misbehavior of nodes can be identified. By using the key pre-distribution the network can be build. All data collected from the previous stages will be finally verify and give to sink. Data loss will be avoided on comparing to existing system. Checking other sensor nodes will avoid traffic and delay.

- Sink. Information got from previous states will finally reach to main location. Here it will be receive securely. Without any delay information will be receive in high secure manner. So that attacker

- cannot take chance of modifying data.

THREE TIER SECURITY

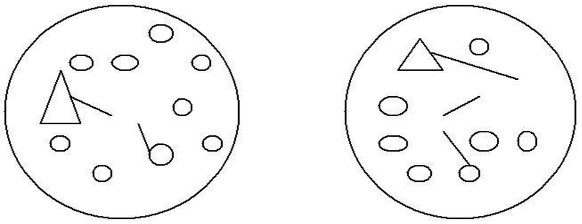


Fig.1: (a) Direct path (b) Indirect path

△ - Sink

□ - Access point

○ - Sensor node

In existing system authentication and polynomial based probabilities were used. The polynomial consists of static and mobile polynomial. The sink will ask for the message to send from below stages. It will have the sensor nodes which are previously chosen called stationary access nodes. The information will pass via these stationary access nodes through the key. Direct key and indirect key discovery through stationary access nodes takes place. Then the requested data which is asked by sink will be transfer via these nodes. By usage of the two key pools which is carrying keys where it involves there is no replication attack. Each node picks up the key from key pool with unique id. It will share at least one common key with their unique id. Polynomial based scheme decreases the pre-distributed information. It utilizes many shares of different forms. The path key between sensor nodes do not have direct path and connected by two or more links. Various probabilities of nodes were calculated both in static and mobile polynomial between the sensor and access nodes versus size. The security approaches make more resilient to mobile sink replication attack in the case of three tiers [2]. On comparing to single polynomial key pool based scheme. On the basis of static and mobile polynomial they conclude about the compromising of mobile polynomials with the access nodes when the nodes are captured. On randomly picking the key polynomials it declare that direct key and indirect key path with the access nodes. The limited energy supply will leads to that every node whether fully involved is not applicable. In this system hash chain algorithm were used. This algorithm uses a one -time key password. It calculates the hash values for every data. It is mainly improving the authentication between sensor nodes by using hash chain algorithm. So that lifetime of key will get lost. .Hence they conclude that there is no possible of third person to alter the data [3]. Data loss will be more so that lifetime of the network will get degraded. Hence the drop tail will be more. This data loss and information which wants to send in secure manner which will be solve by improving the security strength in enhancing three tier securities by adding fourth stage which is called watcher node.

PROPOSED SYSTEM

In this proposed system steps have been improved for sending the data in secure manner. So that packet delivery will be successful as compared to existing system. Data loss will be avoided. This will be happen by adding another stage called watcher node. Before data reaching sink the misbehavior of nodes will be identify and solve. Using random keys data will be passing from one node to another. If a mobile node wants to send data to sink first it has to communicate the watcher node that examines the sensor node and evaluates its trust, then only sensor node will be allowed for transmission which further improves the security of the network [4]. The time will be allocated by watcher node for sending and receiving nodes. Within the specific time if the node does not reach, misbehavior of nodes takes place. Data alteration has been done can be concluded. Malfunction of the nodes will be detect and solve. Hence in proposed work different types of plot will be design. Throughput versus number of nodes will be plot. This throughput will declare about the message delivery in secure way. Packet loss can be overcome by comparing existing. It will compare in both existing and proposed. The plot between power and number of nodes has been takes place. This plot will conclude about the power consumption of the nodes. In proposed system power consumption has been less as compared to three tiers. Time taken for distribution of keys in existing and proposed also will be takes place. Keys will not be loss due to the random keys selection. Efficiency versus number of nodes will be plot. The efficiency will declare about how much the packets sending fast in a manner. The watcher node between nodes will check for link verification. If the data will not pass through the link means it will discover the new route for transmission. Using AODV protocol the link can be verified and route will be generated as per link. The watcher node will activate the path whether the data will be facing any traffic problem and solve this issue with link verification.

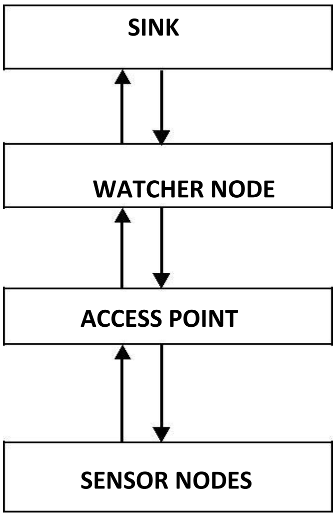


Fig 2: Four tier security

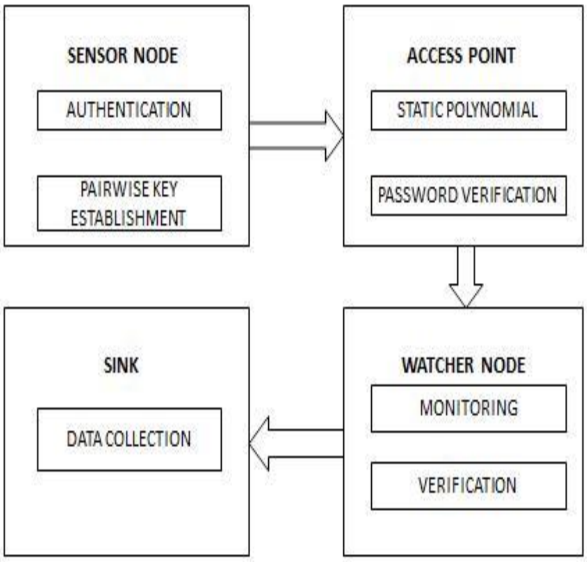
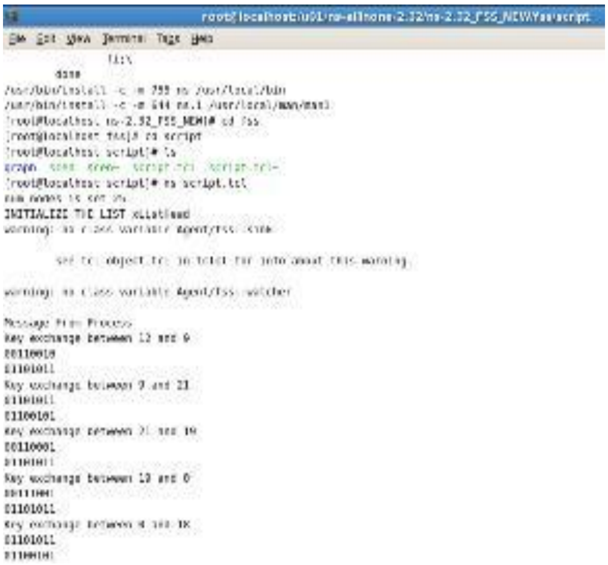


Fig 4: Data flow between the nodes

KEY DISCOVERY

Since in three tier process using the key pools technique such as q-composite key and random pair wise key to improve the security but the pair wise key establishment does not solve. So in four tier security this problem has been solved. Key discovery between the sensor node and access point is the pair wise key establishment [5]. Access point asks for password verification via key establishment. Here the nodes between 12 and 9 is the data between sensor nodes and access point key discovered takes place it as shown in figure. Till the sink, keys generated via the different nodes and watcher node monitor and verify.


root@localhost:/u01/ns-allinone-2.32/ns-2.32_FSS_NEW/fss/script
File Edit View Terminal Tabs Help

```
                fi;\
        done
/usr/bin/install -c -m 755 ns /usr/local/bin
/usr/bin/install -c -m 644 ns.1 /usr/local/man/man1
[root@localhost ns-2.32_FSS_NEW]# cd fss
[root@localhost fss]# cd script
[root@localhost script]# ls
graph  [illegible]
[root@localhost script]# ns script.tcl
num nodes is set 25
INITIALIZE THE LIST xListHead
warning: no class variable Agent/FSS::sink

        see tcl-object.tcl in tclcl for info about this warning.

warning: no class variable Agent/FSS::watcher

Message From Process
Key exchange between 12 and 9
00110010
01101011
Key exchange between 9 and 21
01101011
01100101
Key exchange between 21 and 19
00110001
01101011
Key exchange between 19 and 0
00111000
01101011
Key exchange between 0 and 18
01101011
01100101
```

FIG 3: KEY EXCHANGE BETWEEN THE NODES

FLOW OF DATA

The flow of data will be explained as the following diagram in which for each sensor node how they are communicating with each other for sending and receiving data till it reach the sink.

Transmission between the nodes which is the flow of data in which each data flow will leads to a set of verification and pair wise key management which have to denote. From the sensor node the authentication which have to ask for message whether the data can flow to another stage [6]. It includes pair wise key exchange between the data flows. The access point asks for password verification to determine whether the data which is send from sensor node. Then the watcher will monitor all data which have to pass to the sink. Finally the monitored data will send to the sink in secure manner. Each time the sensor node will communicate via this process for successful transmission and receiving the messages where it is coordinating with each node in each block.

EXPERIMENTAL RESULTS

The following windows will represent about the data collection from sensor nodes to sink.

Sensor node collection

The data which is collecting in sensor nodes which have to send to access point. Hence the collection of sensor nodes will be consists of 25 nodes. Each stage has different nodes. When the data sent from node 12 to node 9, data will be transferred without any loss with the key exchange between them [7]. The random pair wise key will generate the keys and verified by the access point then proceed to access point. In proposed system data loss will be avoided and data will not be resent to the base station by initiating the sensor nodes with the help of stationary access nodes and start to work through the process. Key establishment will be leads to successful transmission of message to access point. Sensors which are used as low power and low cost are enabled with form of transmission .Nodes will be authenticated before the data transmission. Then it will encrypt the data and finally decrypt will takes place.

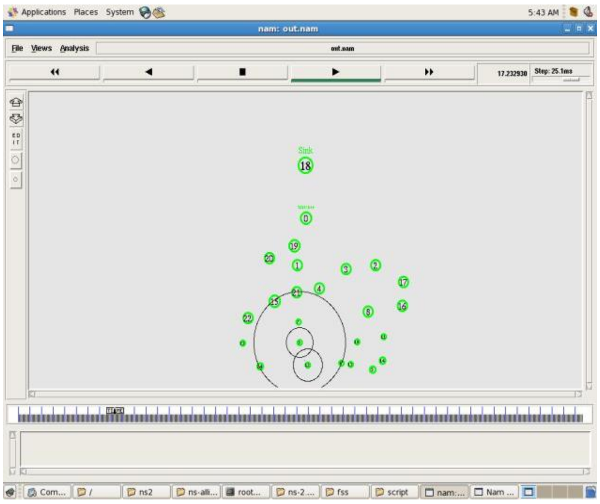


Fig 5: Data collection in sensor nodes

Access point collection

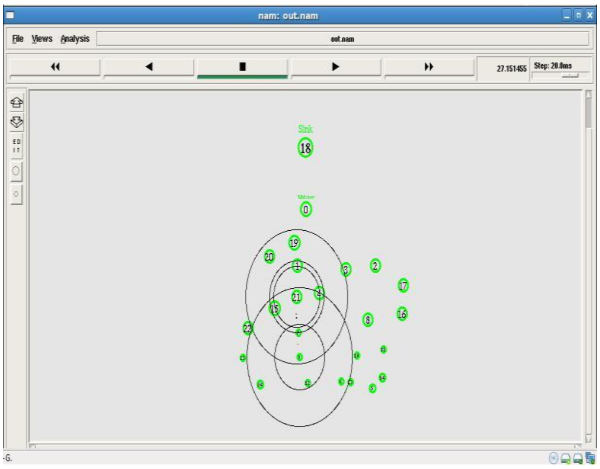


Fig 6: Data collection in access point

The data collected from sensor nodes which will send to access point. The access point will send information to watcher node. Here also between the nodes key will be verified [8]. Here the sink will ask for the message to send and the sensor nodes will initiate this process via stationary access nodes. Then it will proceed to watcher node.

Watcher node collection

The watcher node will get the data from access point will be check for link verification and also generate the keys to verify the password [9]. And also it will monitor the sensor nodes to send data in no traffic manner. Hence it will reduce the energy consumption in base station during long distance when the data transmit.

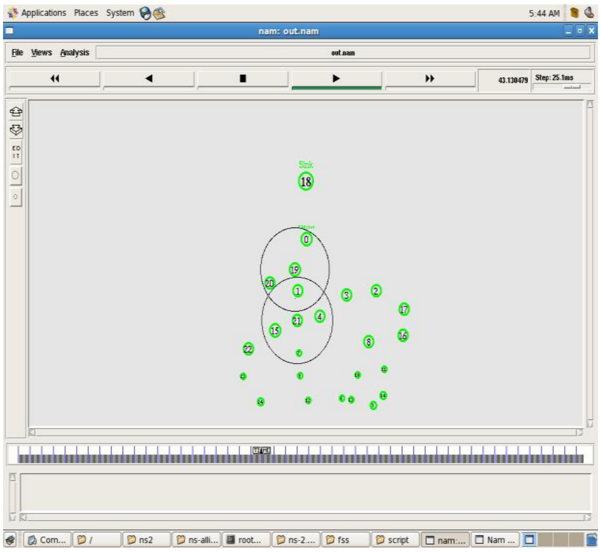


Fig 7: Data collection in watcher

Destination

Hence the data collected in sink through watcher node will be secure in manner. Finally the data reach on the destination will not lost and hence on comparing to existing the throughput will be more and energy also save during this process [10]. And it will be use in all applications such as monitoring the different areas in hazardous environment.

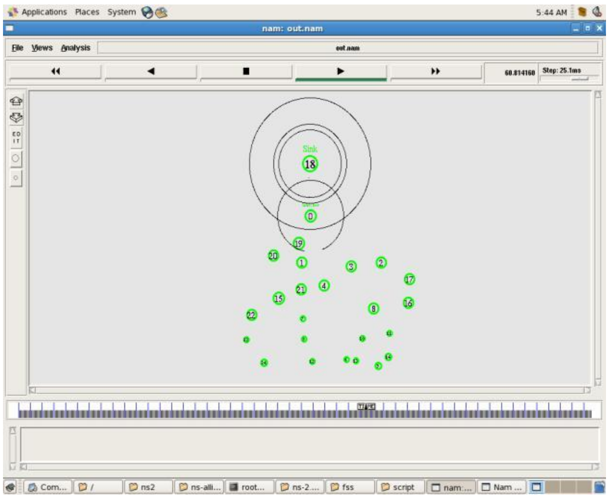


Fig 8: Data collection in sink

Energy versus time

The following figure shows the overall energy in both existing and proposed system. On comparing to existing energy save and leads to reduce the retransmission and packet loss [11]. Here in this energy plot the residual energy has been calculated. The residual energy of average values can be plotted. The average value of residual energy of all nodes of transmission can be plotted. The time will be varying in milliseconds. The point which marked in the graph is the data flow during transmission which is the average residual energy value. So that energy will be save using four tier security. The watcher will save the energy and the base station will not lose the data. The work of base station will be less as compared to existing system.

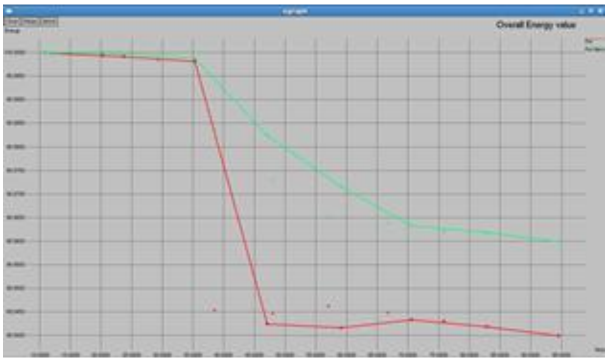


Fig 9: Energy vs. time

Throughput versus time

The plot between throughput and time has compared in existing and proposed. On comparing to existing throughput has been increased in proposed. Delivery of messages will be fast and secure on comparing to three tier. Due to this packet retransmission will be eradicate [12]. Since the watcher monitoring the nodes and verifying any data alteration will leads to the success of delivering messages. The difference between the sending and receiving packets is the throughput value.

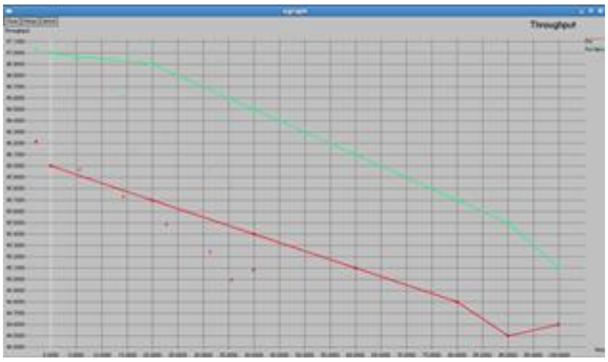


Fig 10: Throughput vs. time

Packet delivery ratio versus time

The total ratio of packet successfully delivered is called packet delivery ratio. The data flow will be in successful manner [13]. All data will have their unique packet identification for delivering the message with respect to the link availability.

The plot between PDR (Packet delivery ratio) and time will conclude that delivering the packets in an efficient manner. The overall efficiency of the network will increase on comparing to three tier [14].

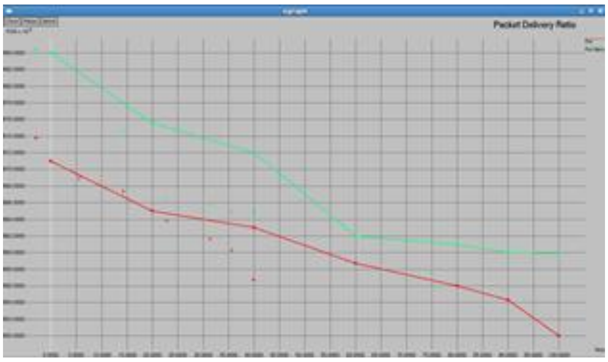


Fig 11: PDR vs. time

Tiers	Throughput (pkt per sec)	PDR (%)	Overall energy (joules)
Three	96	0.971	E99.999819
Four	97	0.984	E99.999919

Table.1. Comparison of three tier and four tier on the basis of performance

The performance of three tier and four tier were compared here. Hence on comparing throughput will be better than three tier. The packet delivery ratio also improved and overall efficiency also well increase on the basis of packets transmission [15]. The overall energy values also mentioned here about the saving in four tier security system as well.

CONCLUSION

In this paper four tier security has been proposed to improve the security levels in different applications. Using the pair wise key and authentication between the sink and sensor nodes well established. Hence using watcher node the performance improved on comparing to three tier and protect against the replication attacks. It leads to improving authentication between the sensor nodes and access point. Also network performance enhanced by minimizing energy consumption and packet transfer rate at node level. Comparison of different parameters has been done. The throughput will be more on comparing to three tier. The residual energy is more than existing. Due to this delay gets reduced in four tier security compared to existing. Packet delivery ratio will be successful in terms of efficiency on comparing to three tier will be more. The simulations which were used here ns2.32. Minimizing the overheads in key generation and verification will be directed towards future work. The proposed technique will increase security level by solving the issues related to keys. The related work will be identifying misbehavior of nodes with random key process towards future work.

REFERENCES

[1] H.chan ,A. perigg and D.song,"Random key pre-distribution schemes for sensor networks," proc. IEEE symp. Research in security and privacy, 2003.

[2] Y.Titra , Z.Li, Y.Lu and S.Bagchi," Efficient collection of sensor data in remote fields using mobile collectors", proc. 13th international conference computer comm. and networks(ICCCN'04), oct 2004.

[3] A.Rasheed & R.Mahapatra, "An energy efficient hybrid data collection scheme in wireless sensor networks", proc. Third international conference on sensor networks and information processing, 2007.

[4] L.Lamport," Password authentication with insecure communication", comm. ACM, vol,24,no.11.pp 770-772.nov 1981.

[5] D.W.Carman, P.S.kurus and B.J.Matt," constraints and approaches for distributed sensor network security,"sep1,2000.NAI labs technical report No.00-010.

[6] W.Du,J.deng,Y.s.Han and P.K.varshney," A pair wise key pre distribution scheme for wireless sensor network," IN ACM CCS 2003, page 42{51,oct.2003}.

[7] Apostolos, pyergelis."Cryptography and security in wireless sensor networks," department of

computer engineering and informatics, 2009.

[8] J.R.Douceur ,” The Sybil attack,”proc. First international workshop peer to peer systems (IPTPS’02). Mar 2002.

[9] D.Liu, P.Ning ,“ Location based pairwise Key Establishments for static Sensor Networks,” wireless Sensor Networks, pp. 277-303, Kluwer academic, 2004.

[10] W. Zhang, G. Cao, and T. La Porta, “Data Dissemination With Ring-Based Index for Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), pp. 305-314, Nov. 2003.

[11] M.Conti, R.D.Pietro, L.V.Mancini and A.Mei,” A Randomized, Efficientand distributed protocol for the detection of node replication attacks in wireless sensor networks,” proc.ACM Mobihop, pp.80-89, sept.2007.

[12] R. Blom, “Non-public key distribution,” In Advances in Cryptology-CRYPTO’82, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. New York: Plenum Publishing, pp.231-236, 1982.

[13] L. Eschenauer and V. D. Gligor, “A keymanagement scheme for distributed sensor networks,” Proc. of the ACM Conference Computer Communication Security(CCS’02), pp. 41-47, 2002.

[14] G. Ahmed, “Impact of Mobile Sink Speed on the Performance of Wireless Sensor Networks,” vol. 1, no. 2, pp. 49–55, 2007

[15] Charles E. Perkins and Elizabeth M. Royer, “Ad-hoc On-Demand Distance Vector Routing,” Proceeding of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’99), New Orleans, LA, USA, February 1999, pages 90-100