EEKWSN –Energy Efficient Key Distribution in Wireless Sensor Network

Ambika.N
Dept of MCA (VTU)
Dayananda sagar college of Engineering,Bangalore
Research Scholar, Bharathiar University

G.T.Raju
DEAN & HOD
Dept. of Computer science and Engineering
RNSIT, Bangalore

ABSTRACT

Wireless sensor network is a field which is spreading its wings into different application areas. Security is the primary concern as these nodes are deployed in unattended and harsh environment. Authentication and integrity of data becomes essential to monitor the network installed in remote areas. This paper generates group keys for every session to encrypt data. The technique minimizes 5.5% of the energy consumption in the network compared to other traditional methods. Backward and forward secrecy is Sybil attack, sinkhole attack and wormhole attack are minimized are tackled in this work.

Keywords

Energy efficient algorithm, group-based authentication key, key distribution, Markov chain

1. INTRODUCTION

Sensor is one of the important entities in the computerized world which has gained a lot of importance. These sensors are tiny devices capable of sensing, processing and providing the reading to the respective authorities. These sensors are usually deployed in remote locations where supervision becomes critical. Hence these sensors have to employ some prevention techniques to combat different types of attacks from the intruders.

The sensors are either placed in hierarchical fashion or are cluster based. In this paper cluster based routing is considered. Authentication among the group members hikes trust among them. This in turn improves integrity of the transmitted data. Key generation and its distribution facilitate completion of both authentication and integrity.

In this paper, group key is generated using Markov chain. The main contribution of this paper is the group key generated is not distributed among the cluster members, which eliminates the load on the cluster head. In addition to saving certain amount of energy, the process also provides authentication and integrity. The work includes detectors which eliminates irrelevant data from the network adding life span to the nodes the network. The study provides better authentication and integrity to data. Section 2 briefs other related work designed by different authors. Section 3 provides the energy consumption model and its advantages in terms of authentication and integrity. Segment 4 provides the simulated results and the work is concluded in section 5.

2. NOTATIONS USED

Table 1. Notations used in the proposed model

Notation	Meaning
N	Network
BS	Base station
N_i	i^{th} node of the network
R	Transmission range
TIME	Global time
S_TIME	Session time distributed by the base station
NO_i	Nonce generated by cluster head
G_i	Group key

3. RELATED WORK

[1] Is a group-based pair-wise key establishment protocol which uses identity- based cryptography. Sensors are deployed in pre-determined pattern. They are pre-distributed with group and individual keys. Provisioning Authority provides unique identity based key to each group. The group has adjacent group's information.

Group key authentication scheme [17] has its base from [16]. Two-dimensional Gaussian distribution is assumed to design the protocol. The sensor nodes which are lying in the neighborhood are likely to have more number of common keys. Discovering shared keys and path key establishment stages follow the same instructions as in [16].

In [18] the author has proposed novel group-based pre-distribution framework which can be combined with the existing key pre-distribution schemes. The nodes are to be grouped and deployed. At the time of deployment the resident node follows probability distribution function. The model implements in-group key pre-distribution method which forms Pair-wise keys. To handle this cross-group pre-distribution method is employed which bridges different deployment groups together.

4. ASSUMPTIONS

4.1.1 Assumption 1

The base station is assumed to be trust worthy. It is the responsibility of the base station to generate group keys and assign unique ids to each node. These nodes are pre-loaded with these keys and deployed either manually by a robot or by thrown from the helicopter into the environment under study. The nodes are pre-grouped by the base station and assigned same group key. Hence after deployment the nodes possessing the same group key tend to cluster into the same group.

4.1.2 Assumption 2

The nodes do not have any prior knowledge of the network. The network is assumed to be free from any kind of attack till the formation of cluster.

4.1.3 Assumption 3

The intruder is assumed to be incapable of generating keys using Marko chain (though it can gain access to the keys if the node gets compromised). If a node is compromised, it either transmits data out of bounds or restricts itself to transmit data. The main intension of the intruder would be to drain out the energy in the network and provide false information to the base station.

5. PROPOSED MODEL

The network is homogeneous consisting of nodes which has to ability to self-configure, form clusters and communicate the necessary data to the sink node. The model is based on Markov chain concept. The cluster members are presumed to generate the different keys for every session. These keys are generated and utilized without any distribution by any single node. The method assures safety of encryption keys and also cuts down the communication cost. These keys are not communicated as in [18] hence the proposed model proves to be much safer.

5.1 System Model

Tinynode 584 configuration is utilized to model the system under study. The node plays the following roles-

5.1.1 Cluster head

The node is responsible to generate nonce and distribute them to the cluster members. They act as detectors verifying the data for their reliability. They remove the redundant data and forward the data to the next available hop/ sink node.

5.1.2 Cluster members

These nodes are deployed to sense the environment, encrypt the sensed data and forward them to the respective cluster head.

5.2 Deployment of Nodes in the Environment

The nodes supposed to be grouped together as a cluster are provided with same group key before deployment. The nodes are embedded with unique id ID_i, group key G_i. After deployment the nodes self-configure. The nodes broadcast HELLO message (as depicted in notation 1). The nodes which are able to receive the transmitted message send back the ACK message. This is represented in notation 2. After authentication, they form a cluster. The base station broadcasts the time and session time (equation (3)) according to which the nodes modify their encryption key.

$$\boldsymbol{N_i \rightarrow N: HELLO} \qquad \textbf{(1)}$$

$$\boldsymbol{N_j \rightarrow N_I: ACK} \qquad \textbf{(2)}$$

$$\boldsymbol{BS \rightarrow N: TIME, S\_TIME} \qquad \textbf{(3)}$$

5.3 Implementation of Markov chain property

Markov chain property is where the states of the Markov chain's present value depend only on the previous value. Equation (4) is the notational depiction of the Markov chain concept.

$$\boldsymbol{P < X_{n+1} = I_{n+1} \;\big|X_n = I_n \ldots\ldots\ldots . X_1 = I_1 >} \qquad \textbf{(4)}$$

After the formation of cluster, the cluster head broadcast nonce to the cluster members. The nodes utilize the group key G_i and nonce NO_i to generate the encryption key (equation (5)) which in turn is used to encrypt the transmission data. The nodes use Markov chain property to generate the encryption key. The data is encrypted using encryption key and transmitted to the cluster head. The cluster head N_C bundles all the data and forwards it to the next hop. The same is represented in equation (6). The redundant data is eliminated by the cluster head. The encryption key E_i is generated for every session.

$$\boldsymbol{E_i \rightarrow ALGORITHM(G_i, NO_i\,)} \qquad \textbf{(5)}$$

The encryption key of the previous session becomes the group key to generate the next encryption key. Care is taken to delete the previous encryption key. The technique provides forward and backward secrecy.

$$\boldsymbol{N_c \rightarrow EN\_DATA(N_i)||\; EN\_DATA(N_j)||\, EN\_DATA(N_k)} \qquad \textbf{(6)}$$

5.4 Role of the detectors

5.4.1 Cluster head

The group head of the cluster behaves as the detector monitoring the activity of the cluster members and filters the irrelevant data. The Intrusion detection system takes the reference of prior knowledge. The assumption is made after a certain observation of the network under study. The data captured are being assembled if it belongs to the cluster under consideration. Rest of the data is termed as outliers.

5.5 Security Analysis

5.5.1 If the Cluster head is compromised

If the cluster head is compromised, it will not be able to generate a nonce and broadcast to the cluster members. After time t, the cluster members report the matter to the base station. The base station keeps cluster head under observation and cluster members are given permission to elect another cluster member as the cluster head.

5.5.2 If any of the Cluster members are compromised:

If the cluster member is compromised, the compromised nodes will either not be able to generate new encryption key or it will not be able to send the encrypted data on time. The cluster head reports the matter to the base station, which in turn concludes the node as compromised after certain observations and remove it from the cluster.

6. SIMULATED RESULTS

The work is simulated using NS2. The surveillance area is 500m*500m. The nodes are being deployed uniformly in the network with each cluster containing 5 cluster members. Summing up the nodes in the network, 100 clusters are being formed. Length of the generated encryption is 132 bits in length and the nonce generated is 4 bits in length.

Table 3 . Parameters used in simulation

parameters	Quantity
Dimension of the network	100m * 100m
Distribution of nodes	uniform
Total number of nodes in the network	500
Number of clusters	100
Number of nodes in the cluster	5 each
Length of the encryption key(group key)	132 bits
Length of nonce generated	4 bits
Length of the group key deployed	132 bits
Tinynode 584 configuration	
Data frame size	272 bits
Acknowledgment frame size	64 bits
Data bit rate	76 kbps
Preamble	6 bytes

6.1 Energy consumption

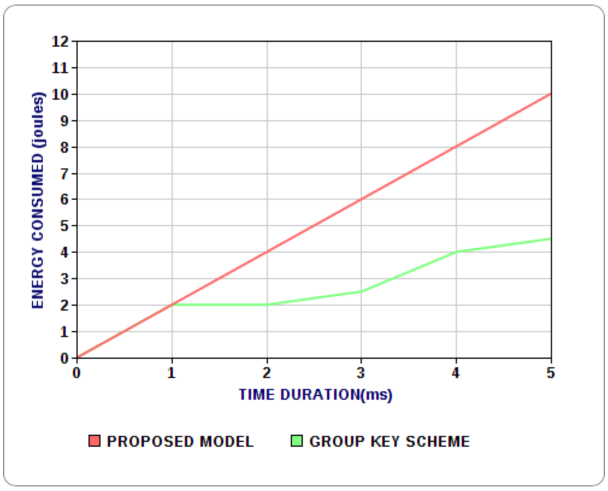

Fig 1. Depiction of Energy Consumption in the network under study

Energy is one of the essential resources in the nodes used to monitor the environment, track any object, and accomplish any other task in the environment. As these nodes are battery powered and can't be recharged, conserving energy becomes priority. Apart from conserving energy the nodes, it should also complete the task undertaken. One of the measures that can be incorporated is using some security measure so that the network containing compromised node is being tackled on time, conserving energy which would have been wasted by the compromised node(its own energy and energy of the nodes which it receives/transmits data). Distributing the keys consumes certain amount of energy at transmitter and receiver end. The proposed model apart from enhancing security also conserves certain amount of energy. It utilizes 5.5% less energy than [18]. The energy is calculated using equation (7). The graphical representation of the work is depicted in fig 1.

$$\mathbf{E_{total}} = \sum_{n=1}^{N}\Big((E_{sampling} * \mathbf{time}) + (E_{transmit} * \frac{\mathbf{no\ of\ frames}}{\mathbf{data\ rate}}) + \mathbf{E_{computation}} \times \mathbf{no\_of\_bits} + (\mathbf{E_{listening}} \times \mathbf{time}) + (E_{receive} * \frac{\mathbf{no\ of\ frames}}{\mathbf{data\ rate}})\Big) \qquad \textbf{(7)}$$

Where

E_{total} – Total energy consumed

$E_{listening}$ - energy consumed in listening

$E_{transmit}$ - energy consumed to transmit data

$E_{receive}$ - energy consumed to receive data

$E_{computation}$- energy consumed used to compute data.

6.2 Sybil attack

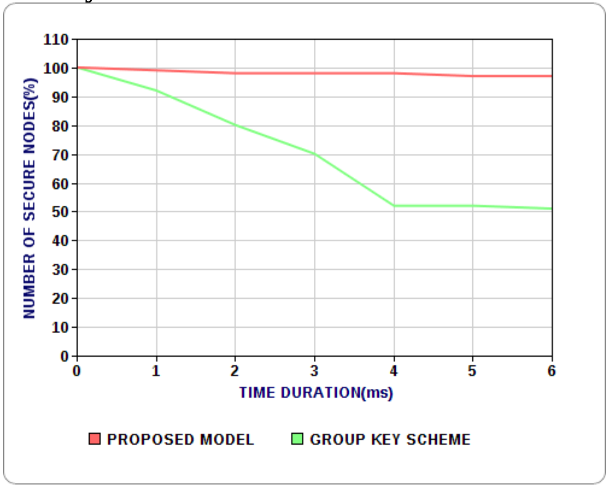

Fig 2. Pictorial Illustration of Sybil attack

Sybil attack [2][3] is where the identities of the nodes are duplicated. The nodes that are compromised and are under the control of adversaries try to duplicate identification. These duplicated nodes gain trust of the neighboring nodes. Trust of the neighbors, serves their purpose. The neighbors can forward the data for transmission to these nodes, disclosing the information. If the compromised node turns to be the cluster head, all the data of the cluster gets accumulated in the compromised node. Hence integrity of the network is put into danger. The encryption keys for every session are changed and this behavior of the network safe guards the data to a larger extent.

In proposed model, the nodes under this kind of attack will not be able to generate the encryption key. The cluster head can behave as a detector tracking the encrypted data. Timely transmission of data using the session key from the node end assures the node as normal node. The graph is plotted for [18] assuming that the intruder can pilfer the encryption keys when the two communicating parties try to find the common keys. From fig 2, simulated results show that there is an increase of 18.8% security against Sybil attack.

6.3 Wormhole attack

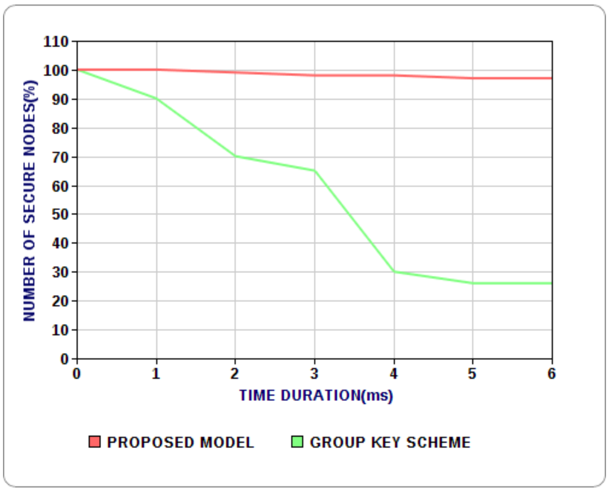

Fig 3. Portrays outcome of Wormhole attack

Wormhole attack [4][5] is where an attacker records the packet at one location in the network, tunnels them to another location and retransmits into the network. The cluster uses different encryption key to encode the data providing better security for the data and helps to control the replay of data to a larger extent. As the encryption keys are changed for every session, the data is safer by 28.2% against wormhole attack. In addition group key is similar to location based keys which indirectly denotes the position of the deployed nodes. Graphical representation of the attack is represented in the fig.3.

6.4 Sinkhole attack

Sinkhole attack [7][8] usually attract the surrounding nodes either by spoofing or replaying the messages, creating an illusion that it is the only one which is extremely high quality route to the base station. In the work, the cluster head authenticates and monitors the nodes in the cluster providing security against the attack. As the encryption keys are not exchanged between the group members and changed time to time, the approach provides 31.8% security against sinkhole attack. The same is portrayed as a graph in fig 4.

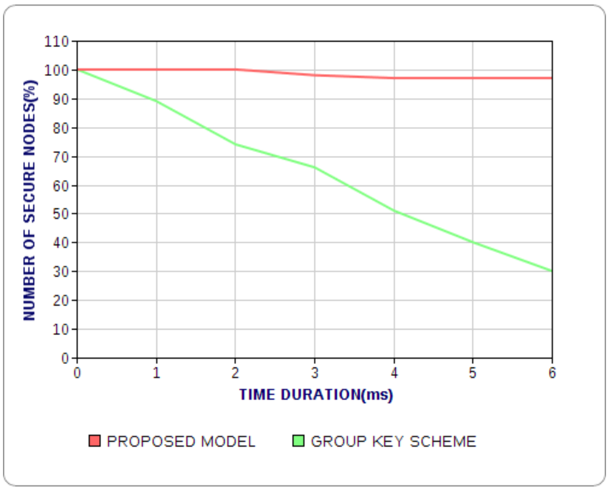

Fig 4. Graphical illustration of Sinkhole attack

Table 4. Results obtained during simulation

Probability values	Proposed Model
Probability of detection of compromised nodes	>=0.75
Probability of false alarm	<=0.5
Probability of data integrity	>=0.72
Probability of reliable data reaching base station	>=0.91

Table 4, provides the results obtained after simulating the study. The work is designed to protect the data from unauthorized users, detect the malicious node and eliminate from the network. The work evaluates the probability to detect compromised nodes, false alarm, data integrity and the reliability of data reaching the sink node.

1 is the optimum value where the network is 100% secure. The work utilizes a group key encryption scheme which alters for every session. The key also indirectly notifies the base station to which location it belongs. This procedure provides 91% of reliable data reaching the base station. The detectors eliminates the data not belonging to the group, cutting down the communication cost and adding an extra to the life span of the nodes.

7. CONCLUSION

Wireless sensor network is an area where huge numbers of nodes are being deployed for multiple/single purpose. These nodes come together to accomplish pre-defined the task. As these nodes are being deployed in harsh environments without any supervision, the attacks by the intruders to hack the data being transmitted. Hence some security measures have to be incorporated as a counter measure to these attacks. This paper generates encryption key for every session and avoids the keys being transmitted from one node to another in the cluster, hence minimizing the consumption of energy during the transmission of encryption key from sender to receiver both ways. The work takes care of nodes from Sybil, sinkhole and wormhole attacks providing a better security to the network.

8. REFERENCES

[1] William R.Claycomb , Dongwan Shin, “A novel node level security policy framework for wireless sensor networks”, Journal of Network and Computer Applications 34 (2011), 418– 428.

[2] James Newsome , Elaine Shi, Dawn Song ,Adrian Perrig, “Detecting Sybil attacks in Wireless Sensor Networks using neighbouring information”, Proceedings of the 3rd international symposium on Information processing in sensor networks, ACM New York, 2004.

[3] Misra.S, Myneni, S. ,”On Identifying Power Control Performing Sybil Nodes in Wireless Sensor Networks Using RSSI“,IEEE Global Telecommunications Conference, 2010.

[4] Yih-Chun Hu, Perrig, A. and Johnson, D.B, “Wormhole attacks in wireless networks “, IEEE Journal on Selected Areas in Communications, Volume: 24 Issue:2 ,370 – 380.

[5] Zhibin Zhao; Bo Wei, Xiaomei Dong, Lan Yao and Fuxiang Gao, “Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis “, WASE International Conference on Information Engineering (ICIE), 2010, 251 - 254.

[6] Liping Teng; Yongping Zhang, “SeRA: A Secure Routing Algorithm Against Sinkhole Attacks for Mobile Wireless Sensor Networks”, Second International Conference on Computer Modelling and Simulation, 2010, 79 - 82.

[7] Changlong Chen, Song, Min, Hsieh and George, “Intrusion detection of sinkhole attacks in large scale wireless sensor networks”, IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010 , 711 - 716.

[8] Denning, D., “An Intrusion Detection Model”, IEEE Transactions on Software Engineering, 1987, 13(2):222—232.

[9] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, Proceedings of the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking, 2000.

[10] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks", IEEE Wireless Communications, Feb 2004,vol. 11, no. 1, 48-60.

[11] Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," ACM MOBICOM, 2000.

[12] Abbasi, A. A. & Younis, M. , A survey on clustering algorithms for wireless sensor networks, Comput. Commun. , 2007, 30(14-15): 2826–2841.

[13] Djenouri, D., Khelladi, L. & Badache, A. ,A survey of security issues in mobile ad hoc and sensor networks, IEEE Communications Surveys Tutorials, 2005, 7(4): 2 – 28.

[14] Roman, R., Applying intrusion detection systems to wireless sensor networks, in CCNC Proceeding of the 3rd IEEE Consumer Communications and Networking Conference, 2006, 640–644.

[15] Wang, Y., Attebury, G. & Ramamurthy, B. , A survey of security issues in wireless sensor networks, IEEE Communications Surveys Tutorials, 2006., 8(2): 2 –23.

[16] Eschenauer L, Gligor V, “A key management scheme for distributed sensor networks”, In Proceedings of the Annual ACM Computer and Communications Security (CCS), 2002.

[17] Du W, Deng J, Han YS, Chen S, Varshney PK. A key management scheme for wireless sensor networks using deployment knowledge, In Proc. of the 24th IEEE Conference on Computer Communications (INFOCOM), 2004.

[18] Liu D, Ning P, Du W. Group based key pre-distribution for wireless sensor networks. ACM Transactions on Sensor Networks (TOSN) 2008.