International Journal of Computational Intelligence and Informatics, Vol. 1 : No. 1, April - June 2011

Energy Efficient Cluster based Key Management & Authentication Technique for Wireless Sensor Networks

T. Lalitha
Research Scholar,
Bharatiar University, Coimbatore,
Tamilnadu, India
lalithasrilekha@rediffmail.com

R. Umarani
Department of Computer Science,
Sri Sarada college for women, Salem.,
Tamilnadu, India
umainweb@gmail.com

Abstract

In wireless sensor networks, the security attacks are due to the compromise of the large part of the network which can cause node damage or disturbance in the data flow. At the time of re-keying process, if the re-key from the sink is not securely transmitted to the compromised node, it will lead to denial of service attack. In this paper, we propose a cluster based key management technique for authentication in wireless sensor networks. Initially, clusters are formed in the network and the cluster heads are selected based on the energy cost, coverage and processing capacity. The sink assigns cluster key to every cluster and an EBS key set to every cluster head. The EBS key set contains the pairwise keys for intra-cluster and inter-cluster communication. The cluster head upon detecting a compromised node in its cluster sends a request to sink to perform re-keying operation. The re-keying process utilizes the hashing function for authentication and nodes are recovered in a secured manner. During data transmission towards the sink, the data is made to pass through two phases of encryption thus ensuring security in the network. By simulation results, we show that the proposed approach recovers the compromised node in the secured manner.

Keywords: wireless sensor networks, Cluster key, NS2.

1. Introduction

1.1 *Wireless sensor networks*

A network comprising of several minute wireless sensor nodes which are organized in a dense manner is called as a Wireless Sensor Network (WSN). Every node estimates the state of its surroundings in this network. The estimated results are then converted into the signal form in order to determine the features related to this technique after the processing of the signals.

Based on the multi hop technique, the entire data that is accumulated is directed towards the special nodes which are considered as the sink nodes or the Base Station (BS). The user at the destination receives the data through the internet or the satellite via gateway. The use of the gateway is not very necessary as it is reliant on the distance between the user at the destination and the network [1].

1.2 Authentication in sensor networks

The secured communication can be realized using user authentication concept. This constitutes three phases that are described as follows :

Registration Phase: The user ID and password of the user is submitted to gateway node.

Login Phase: The user ID and password is submitted to the login node

Authentication Phase: The user and timestamp's validity is verified by the gateway node.

2. Proposed Work

The several security attacks prevailing in the sensor networks can cause the destruction of the nodes or interruption in the data flow. As the base station can detect nodes that are forwarding the anomalous data, attacks are typically based on the compromise of a large part of the network. During the recovery operation, the messages from the base station which is requesting re-keying operation is required to be authenticated. Otherwise it can result in denial of service attack. Thus, we propose to design a cluster based authentication technique for wireless sensor network. The public key cryptography is used when there is large number of user due to its scalability. Since public key cryptography is more power consuming sensor communicates among each other with the help of symmetric cryptography. Thus the sensors in the communication range serve as promoters between public key cryptography of the user and symmetric crypto world of WSN. The user communicates to sensors with the help of public key cryptography and sensors communicate to the rest of the

sensor network using symmetric cryptography and this process occurs in authenticate manner as follows.

i. The initialization of robust secure channel among user and WSN.
ii. Forwarding the authenticated queries [2].

3. Authentication Technique

When the cluster head (CH) has found that one of the members in its cluster is compromised or captured, it requests the sink to implement the re-keying operation. The steps involved in the re-keying process are as follows.

a) CH retrieves the ID of the node (say v) requiring re-keying.

b) CH XORs the ID, its own secret K_{CH}, the request for re-keying message G_{req} and the time T to obtain the message G. It is represented as (ID $\otimes K_{CH} \otimes G_{req} \otimes$ T)

c) CH computes hash value of the XORed data represented as d. i.e. d = H(ID $\otimes K_{CH} \otimes G_{req} \otimes$ T)

d) CH sends the computed hash value d, node ID, G_{req} and T to the sink.

e) The sink retrieves K_{CH} and re-computes the hash value which is given as f. The computed hash value is compared with d.

f) Upon comparison, if it is found that d is equivalent to f, and the time T is not utilized in a re-keying process previously, then the sink performs the subsequent steps.

g) The sink XORs the pairwise key P_{ij}, the re-keying message G_{req} and time T to obtain G. i.e. ($P_{ij} \otimes G_{req} \otimes$ T).

h) The sink then computes the hash value of P_{ij}, G_{req} and T. i.e. H($P_{ij} \otimes G_{req} \otimes$ T) = p.

i) The sink sends p, G_{req} and T to CH.

j) The CH re-computes hash value of XOR of v with P_{ij}, G_{req} and T which is represented as b and compares it with p. Upon comparison, if it is found that b=p and the time T has not been utilized in a re-keying process previously, the re-key P_{ij} is sent to the affected node and it is re-keyed.

The node updates its secret to P_{ij} = G and informs the sink that it has successfully re-keyed and the sink then updates the node's secret in its table.

4. Simulation Results

The proposed Energy Efficient Cluster Based Key Management and Authentication (EECBKMA) technique is evaluated through NS2 simulation. We consider a random network of 100 sensor nodes deployed in an area of 500 X 500m. Two sink nodes are assumed to be situated 100 meters away from the above specified area. In the simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The simulated traffic is CBR with UDP. The number of clusters formed is 9. Out of which, we transmit data from 4 cluster heads to the sink. 3 sensor nodes in each cluster are sending data to their cluster head. The attacker nodes are varied from 2 to 10. Table 1 summarizes the simulation parameters used for this study.

Table 1. Simulation Parameter

No. of Nodes	100
Area Size	500 X 500
Mac	802.11
Routing protocol	EECBKMA
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 bytes
Rate	250kb
Transmission Range	250m
No of clusters sending data	1,2,3 and 4
No. of nodes per cluster sending data	3
Transmit Power	0.395 w
Receiving power	0.660 w
Idle power	0.035 w
Initial Energy	17.1 Joules
No. of Attackers	2,4,6,8 and 10

5. Performance Metrics

The performance of EECBKMA technique is compared with the SecLEACH [3] scheme. The performance is evaluated mainly, according to the following metrics.

5.1 Average Packet Drop

The number of packets dropped due to various attacks is averaged over all surviving data packets at the destination.

5.2 *Average Packet Delivery Ratio*

It is the ratio of the number of packets received successfully and the total number of packets transmitted.

5.3 Energy

It is the average energy consumed for the data transmission.

6. Results

6.1 Based on Attackers

In our initial experiment, we vary the number of attackers as 2,4,6,8 and 10 from various clusters performing node capture attacks.

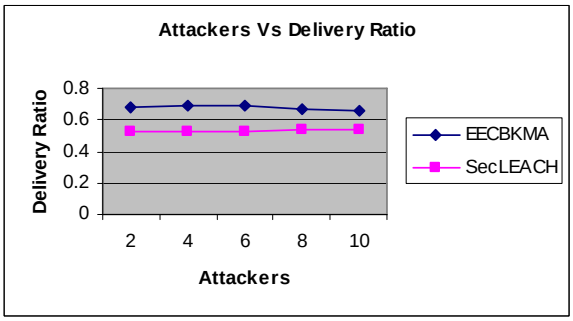

Fig. 1 Attackers Vs Delivery Ratio

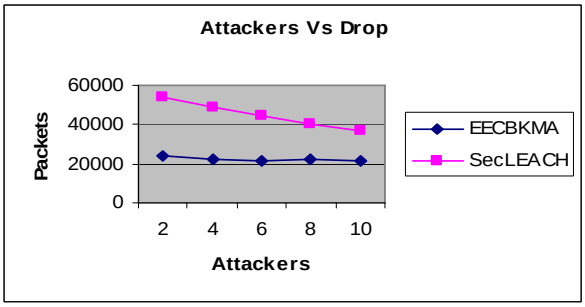

Fig. 2 Attackers Vs Drop

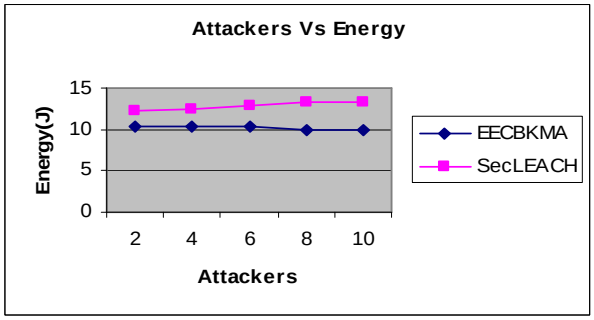

Fig. 3 Attackers Vs Energy

When the number of attackers is increased, naturally the packet drop will increase there by reducing the packet delivery ratio.

Since EECBKMA reduces node capture attacks, the amount of packet drop is less, when compared with the existing schemes. Fig. 1 and Fig. 2 give the packets drop and packet delivery ratio when the attackers are increased. It shows that our proposed EECBKMA technique achieves good packet delivery ratio with less packet drop when compared to SecLEACH scheme.

Since the cluster heads are selected based on the energy cost, the overall energy consumption is less in EECBKMA. Fig. 3 gives the energy consumption when the number of attackers is increased. It shows that our proposed EECBKMA technique utilizes lower energy when compared to SecLEACH.

6.2 Based On Various Cluster Sizes

In this experiment we vary the cluster size from 1 to 5. Sensor nodes in each cluster are 3 which are sending data to their cluster head, which are forwarded to the sink. The attacker nodes are kept as 2.

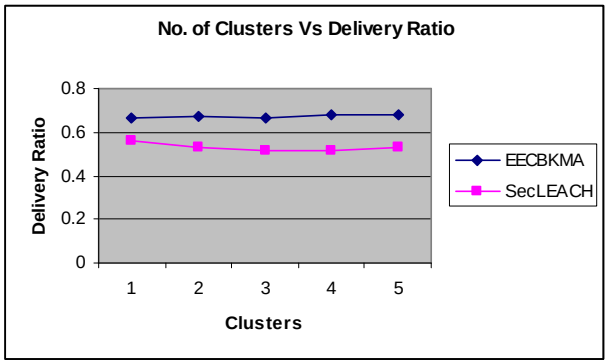

Fig. 4 Clusters Vs Delivery Ratio

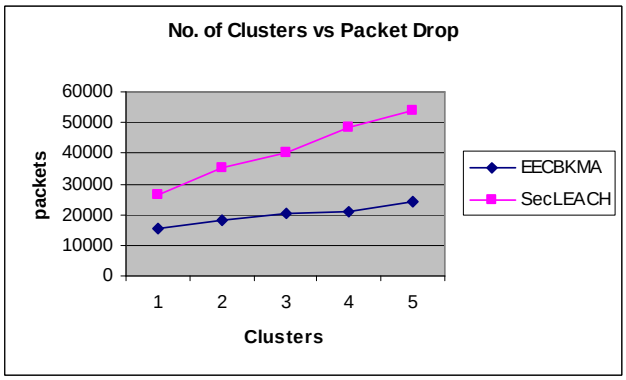

Fig. 5 Clusters Vs Packet Drop

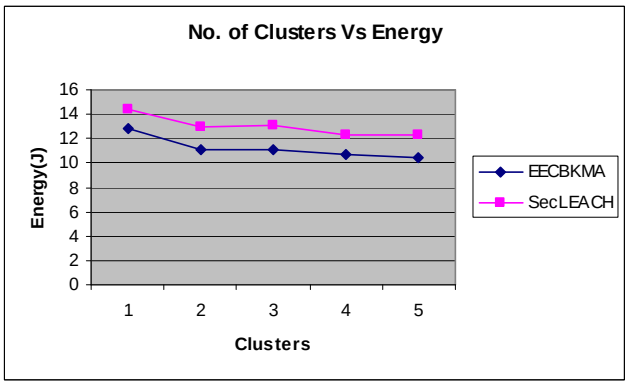

Fig. 6 Clusters Vs Energy

Fig. 4 and Fig. 5 give the packets drop and packet delivery ratio when the cluster size is increased. It shows that our proposed EECBKMA technique achieves good packet delivery ratio with less packet drop when compared to SecLEACH scheme.

Fig. 6 gives the energy consumption when the number of clusters is increased. It shows that our proposed EECBKMA technique utilizes lower energy when compared to SecLEACH.

7. Conclusion

In this paper, we have proposed a cluster based key management technique for authentication in wireless sensor networks. Initially, clusters are formed in the network and the cluster heads (CHs) are selected based on the energy cost, coverage and processing capacity. The sink assigns cluster key to every cluster and an EBS key set to every cluster head. The EBS key set contains the pairwise keys for intra-cluster and inter-cluster communication. The cluster head upon detecting a compromised node in its cluster sends a request to sink to perform re-keying operation. The CH retrieves the ID of the node that needs re-keying and hashing function is utilized for recovering the node in the secured manner. When the re-keying is performed successfully, the respective node updates its secret key and notifies the sink that it is been re-keyed. Then the sink updates the nodes secret in its table. During data transmission towards the sink, the data is made to pass through two phases of encryption thus ensuring security in the network. By simulation results, we have shown that the proposed approach recovers the compromised node in the secured manner.

References

[1] Lina M. Pestana Leão de Brito and Laura M. Rodríguez Peralta, “An Analysis of Localization Problems and Solutions in Wireless Sensor Networks”, Polytechnical Studies Review, 2008, Vol VI, ISSN: 1645-9911.

[2] Binod Vaidya, Min Chen and Joel J. P. C. Rodrigues, “ Improved Robust User Authentication Scheme for Wireless Sensor Networks”, Fifth IEEE Conference on Wireless Communication and Sensor Networks (WCSN), pp1 – 6, 2009.

[3] Benenson, Z., Gedicke, N., and Raivio, O, “Realizing Robust User Authentication in Sensor Networks. In Proceedings of Workshop on Real-World Wireless Sensor Networks (REALWSN 2005), Sweden, June 2005.

T. Lalitha received a Master’s Degree in Computer Applications in 2000 in Vysya College,Salem and received a M.Phil(CS) in 2004 Bharathidasan University, Trichy. She now doing Ph.d Part-Time in Bharatiar University, Coimbatore. She is also working as a Senior Assistant Professor in Department of MCA in Sona College of Technology, Salem. Her research interests include network security, network Simulation as well as validation and verification techniques. She has Published 14 Papers in National and International Journals.

R. UmaRani has completed her M.C.A., from NIT, Trichy in 1989. She did her M.Phil from Mother Teresa University, Kodaikanal. She received her Ph.D., from Periyar University, Salem in 2006. Her area of interest includes information security, data mining and mobile communications. She has published about 50 papers in national and international conferences. She is also working as Associate Professor in the Department of Computer Science, Sri Sarada college for women, Salem. She has Published 35 Papers in International and National Journals and 55 Papers in National and International Conferences.