ENERGY EFFICIENT CLUSTER BASED KEY MANAGEMENT TECHNIQUE FOR WIRELESS SENSOR NETWORKS

T. Lalitha[1] and R. Umarani[2]
[1]Research Scholar, Bharatiar University, Coimbatore, Tamilnadu, India
[2]Research Supervisor, Bharatiar University, Coimbatore, Tamilnadu, India

ABSTRACT
Wireless Sensor Networks (WSN) is vulnerable to node capture attacks in which an attacker can capture one or more sensor nodes and reveal all stored security information which enables him to compromise a part of the WSN communications. Due to large number of sensor nodes and lack of information about deployment and hardware capabilities of sensor node, key management in wireless sensor networks has become a complex task. Limited memory resources and energy constraints are the other issues of key management in WSN. Hence an efficient key management scheme is necessary which reduces the impact of node capture attacks and consume less energy. In this paper, we develop a cluster based technique for key management in wireless sensor network. 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. 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 our proposed technique efficiently increases packet delivery ratio with reduced energy consumption.

KEYWORDS: *Wireless Sensor Networks, Key Management, Data Transmission, Attacks, Cluster*

I. INTRODUCTION

1.1 Wireless Sensor Network

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].

For supervising the physical world, the wireless sensor networks are the promising technology. In order to collect the data from the surrounding in a sensor network application, several minute sensor nodes are organized and collaborated. Sensing modals like image sensors are placed in every node and this possess the ability to communicate in the wireless environment [2].

II. ENERGY EFFICIENT CLUSTER BASED KEY MANAGEMENT TECHNIQUE

2.1 Cluster Formation

In the wireless sensor network, after the nodes are deployed in the physical environment, they first report to the base station their physical locations, and then the network starts to select cluster heads.

According to the cluster head selection algorithm, each node decides if it is capable of serving as a cluster head based on the following selection criteria:

a) High Energy Resources
b) Wide Communication Range
c) High Processing Capacity

For the authentication process, the encryption mechanism is carried on.
When the selection criteria are satisfied by a particular node, it is capable of being the cluster head. So, this node, N_i broadcasts a Cluster head beacon (CH_BEACON) packet. The CH_BEACON packet is encrypted with a key called as the primary key, K_{pri}.

$$N_i \xrightarrow[K_{pri}(CH\_BEACON)]{} \text{broadcast}$$

When the neighboring nodes S_i receive this message, a cluster head reply (CH_REPLY) message is sent to the node, N_i by the nodes which intend to join the cluster. The reply message contains the ID and the response content Ack.

$$N_i \xleftarrow[K_{pri}(\ ID\{S_i\} \| \ Ack)]{CH\_REPLY} S_i$$

If the number of reply messages received by N_i is greater than a threshold R_{th}, then N_i can be selected as the cluster head, CH.
If the number of reply messages received by N_i is greater than a threshold R_{th}, then N_i can be selected as the cluster head, CH.
Finally, the cluster head assigns IDs to all its member nodes that intend to join the cluster.

III. EBS CONSTRUCTION

An EBS consists of several subsets of the member set collection. In the EBS, every subset is analogous to a particular key and the nodes which possess the key become the element of the subset. The dimension of the EBS is represented by (N, K, M) and it depicts a condition of a N membered secure group with numbering from 1 to N and a separate key is maintained for every subset by the key server. In EBS, if there exists a subset A_i, then every member of this subset will have knowledge about the key K_i. In EMS, there are M elements for every t € [1, N] and its union is equal to [1, N] – {t}. Hence, any member t can be ejected by the key server. Then re-keying is performed to enable every member to know the replacement keys for the K keys.
To perform this, the M messages are multicast after encrypting them with the keys which correspond to the M elements, which has a union equal to [1, N] – {t}. To restrict decipherability to selected members, encryption of every key is performed by its predecessor.
A canonical enumeration technique is made use of, for the construction of EBS subsets. In the formation of subset of K objects out of K + M object set, every feasible method is taken into consideration. Matrix A is formed in order to develop a bit string sequence in its canonical (K, M), in which the K and M are already known, C (K + M, K) columns indicate the successive bit strings of which has a length of K+M objects, where K ones are present in each. For EBS (N, K, M), "A" is known as the canonical matrix.
For instance, the canonical matrix A for EBS(8, 3, 2) enclose the enumeration of all C(5, 3) ways to form a subset of 3 keys from 5 keys, as shown in Table 1.

Enumeration matrix for EBS(8,3,2)

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
T1	0	0	0	0	1	1	1	1	1	1
T2	0	1	1	1	0	0	0	1	1	1
T3	1	0	1	1	0	1	1	0	0	1
T4	1	1	0	1	1	0	1	0	1	0
T5	1	1	1	0	1	1	0	1	0	0

Every row in the table corresponds to a subset Ti after the construction of the matrix A, where an entry 1 in the row indicates that the corresponding node is present in the subset. Since N = 8, M9 and M10 are not useful, in Table 1, T1 = [5, 6, 7, 8], T2 = [2, 3, 4, 8], T3 = [1, 3, 4, 6, 7], T4 = [1, 2, 4, 5, 7], and T5 = [1, 2, 3, 5, 6, 8]. It is easy to prove:
[1,8] – [1] = T1 U T2,
[1,8] – [2] = T1 U T3,
[1,8] – [3] = T1 U T4,
…
Hence, on the exit of any node in the network information about the keys will be updated only by two node subsets. In this protocol, only five management keys are necessary whereas 15 keys are necessary in case of LKH. This in turn minimizes the key computation and also saves space for storage.
During the construction of the EBS(N, K, M) model in this protocol, the values of the parameters N, K and M are raised in order to facilitate the production of larger number of management keys. Later on, the spare keys are used for the new nodes of the cluster

IV. SIMULATION RESULTS

The proposed Energy Efficient Cluster Based Key Management (EECBKM) 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

No. of Nodes	100
Area Size	500 X 500
Mac	802.11
Routing protocol	EECBKM
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

4.1 Performance Metrics

The performance of EECBKM technique is compared with the SecLEACH scheme. The performance is evaluated mainly, according to the following metrics.

- **Average Packet Drop:** The number of packets dropped due to various attacks is averaged over all surviving data packets at the destination.
- **Average Packet Delivery Ratio:** It is the ratio of the number .of packets received successfully and the total number of packets transmitted.
- **Energy:** It is the average energy consumed for the data transmission.

V. RESULTS

5.1 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.

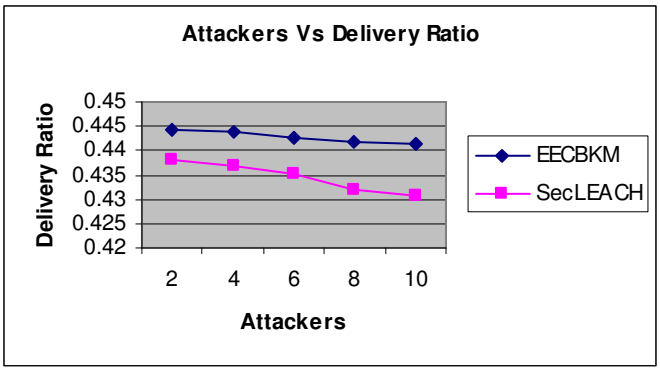

Figure 3: Attackers Vs Delivery Ratio

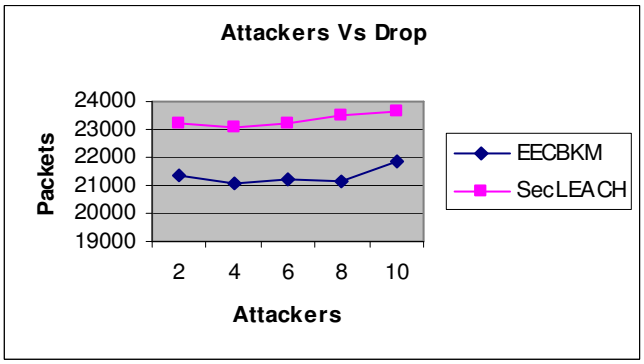

Figure 4: Attackers Vs Packet Drop

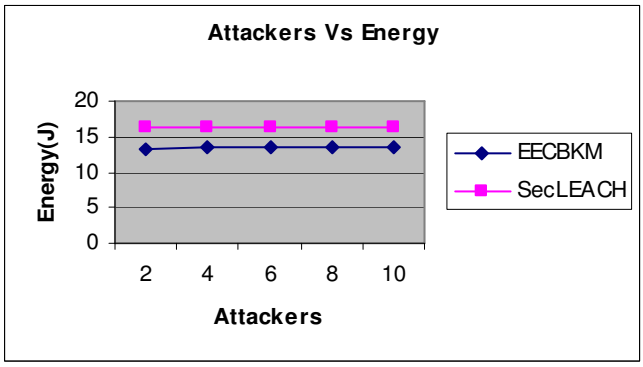

Figure 5: Attackers Vs Energy

When the number of attackers is increased, naturally the packet drop will increase there by reducing the packet delivery ratio. Since EECBKM reduces node capture attacks, the amount of packet drop is less, when compared with the existing schemes. Figure 3 and 4 give the packets drop and packet delivery ratio when the attackers are increased.

VI. CONCLUSION

In this paper, we have developed an efficient technique for key management in the wireless sensor network. During the formation of a cluster, initially a cluster head is selected based on eligibility criteria such as energy cost, coverage and processing capacity. After the cluster head selection, the

information about all the members of the cluster is sent to the sink by the cluster head. The sink then provides the cluster head with the cluster key and the EBS key set required for the communication between the nodes. These keys are distributed to the nodes by the cluster head prior communication. After the key distribution, secure channel is established between the nodes and the cluster head. During the data transmission from the cluster members to the sink, the data passes two phases. In the first phase the data is encrypted and transmitted to the cluster head. In the second phase, the data is encrypted by another key by the cluster head and then transmitted to the sink. Thus this technique allows inter cluster as well as intra cluster communication in a very efficient manner with high security. By simulation results, we have shown that our proposed technique efficiently increases packet delivery ratio with reduced energy consumption.

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]. Huang Lee and Hamid Aghajan, "Collaborative Self-Localization Techniques for Wireless Image Sensor Networks", In Proc. of Asilomar Conf. on Signals, Systems and Computers, Oct. 2005.

[3]. D.Saravanan , D.Rajalakshmi and D.Maheswari "DYCRASEN: A Dynamic Cryptographic Asymmetric Key Management for Sensor Network using Hash Function", International Journal of Computer Applications (0975 – 8887) Volume 18– No.8, March 2011

[4]. Yoon-Su Jeong, and Sang-Ho Lee "Secure Key Management Protocol in the Wireless Sensor Network", International Journal of Information Processing Systems, Vol.2, No.1, March 2006.

[5]. Mohammed A. Abuhelaleh and Khaled M. Elleithy "SECURITY IN WIRELESS SENSOR NETWORKS: KEY MANAGEMENT MODULE IN SOOAWSN", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.

Authors:

Lalitha. T 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 and published a Book "Problem Solving Techniques.

UmaRani. R. 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 topic for research was information security. Her area of interest includes information security, data mining and mobile communications. She has published about 50 papers in national and international conferences. She has produced 20 M.Phil., (Computer Science) candidates. She is currently guiding 5 Ph.D., (Computer Science) research scholars. 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 Ntional Journals and 55 Papers in National and International Conferences.