Cluster based Efficient Key Management and Authentication Technique for Wireless Sensor Networks

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

ABSTRACT
To achieve security in wireless sensor networks, it is important to be able to encrypt messages sent among sensor nodes. Keys for encryption purposes must be agreed upon by communicating nodes.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. By simulation results, we show that the proposed approach recovers the compromised node in the secured manner.

1. SECURITY IN SENSOR NETWORKS
In wireless channels, the communication is not completely secure and is subjected to security hazard. In the wireless channels, the possible security threat can be divided into two threats: inside threat and outside threat. In case of outside threat in the sensor network, the attacker does not possess control over the cryptographic materials. Whereas in case of the inside threat, the attacker will be possess some key materials and trust of some sensor nodes.

Compromising the sensor nodes is an easy task due to the absence of the expensive tampering resistant hardware. Even if it possesses the tampering resistant hardware, it may be very reliant. Modification, forging and discarding the messages is possible in case of a compromised node [1].

In vulnerable locations, maintaining the security of the sensor nodes is a major task. In WSN, the encoding and the authentication of the communication carried out is necessary, to ensure security. For communication between the sensor nodes, few solutions have been developed to attain stability in communication. Distribution key method, dissymmetric encryption method, and key predisposition method are the three kinds of key management techniques [3]. The attacks like jamming and spoofing are very destructive to the sensor networks. Whenever the cluster heads are responsible for the transmission and reception of the data, this nature of the Cluster Hierarchy distribution networks makes it susceptible to destructive networks. So, the network will get destructed if a hacker tries to become the cluster head of the cluster. Examples of this type of attack are the selective forwarding and the sinkhole attacks [2].

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 [4].

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.

3. CLUSTER BASED KEY MANAGEMENT TECHNIQUE

3.1 Intra Cluster Communication
The CH decrypts the pairwise keys sent by the sink, with its cluster key K_{CH} and distributes them to its cluster members.

$$CH_i \xrightarrow{P_{ij}} \{CM\}_j$$

where i = 1 --→ j = 1 to 7

i = 2 --→ j = 8 to 14

i = 3 --→ j = 15 to 21

Where CM are the cluster members.
After the pair wise keys are distributed by the CH to its members, for the establishment of the secure channels between the CH and the cluster members, the CH sends a hello message to the cluster members. Based on the reception of the Acknowledgement message from its members, the CH establishes a channel between itself and its members.

CH_i —Hello message→ $\{CM\}_j$

CH_i ←Ack message— $\{CM\}_j$

CH_i ←Secure channel→ $\{CM\}_j$

where i = 1 --→ j = 1 to 7

i = 2 --→ j = 8 to 14

i = 3 --→ j = 15 to 21

CH_1 —K_{11}→ $\{CM\}_1$

CH_1 —K_{15}→ $\{CM\}_5$

Next a secure path is established between the two nodes; node 1 and node 5 after the exchange of hello message and acknowledgement message.

CH_1 —Hello message→ $\{CM\}_1$

CH_1 —Hello message→ $\{CM\}_5$

CH_1 ←Ack message— $\{CM\}_1$

CH_1 ←Ack message— $\{CM\}_5$

After receiving the acknowledgement message, a secure channel is set up between the node and the CH. Thus through the CH, a continuous path is established between the two nodes that need to communicate with each other.

CH_1 ←Secure channel→ $\{CM\}_1$

CH_1 ←Secure channel→ $\{CM\}_5$

$\{CM\}_1$ ←Secure channel→ $\{CM\}_5$

This technique allows secure communication between intra cluster nodes as well as inters cluster nodes.

3.2 Inter cluster Communication

Whenever a node within a cluster wants to communicate with a node belonging to another cluster then the inter cluster communication takes place in the network. For communication between two clusters, the CH uses the pairwise keys, $PH_{ii'}$ obtained from the EBS key set.

CH_i —$PH_{ii'}$→ $CH_{i'}$

where i = 1, 2, 3; i'= 1, 2,3 and $i \neq i'$

After the distribution of the pairwise keys between the CHs, the secure channels are established between the CHs. Initially the source CH sends a hello message to the CH with which the former wants to communicate. On reception of the Acknowledgement message from the target CH, the source CH establishes a channel between itself and the target CH.

CH_i —Hello message→ $CH_{i'}$

where i = 1,2,3; i' = 1,2,3 and $i \neq i'$

CH_i ←Ack message— $CH_{i'}$

where i = 1,2,3; i' = 1,2,3 and $i \neq i'$

CH_i ←→ $CH_{i'}$

where i = 1,2,3; i'= 1,2,3 and $i \neq i'$

For example, if node 10 of C2 wants to communicate with node 15 of C3, then the following sequence of steps will take place.

Initially the CH2 distributes the pairwise key K_{210} to the node10 and CH3 distributes the pairwise key K_{315} to node 15 and. Then a secure channel is established in C2 between CH2 and node10 and in C3 between CH3 and node15.

In order to establish a secure channel between C2 and C3, the following steps are followed:

CH_2 —K_{23}→ CH_3

Next the hello message is sent by C2 to C3

CH_2 —Hello message→

CH_2 ←Ack message—

On receiving the acknowledgement message, a secure channel is established between the C2 and C3.

CH_2 ←Secure channel→ CH_3

Then through CH2 and CH3, the node10 of C2 and node15 of C3 are connected to each other to form a secure path.

Secure channel

$\{CM\}_{10}$ ⟷ $\{CM\}_{15}$

4. 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.

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

2) 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 ⊗ K_{CH} ⊗ G_{req} ⊗ T)

3) CH computes hash value of the XORed data represented as d.

i.e. d = H(ID ⊗ K_{CH} ⊗ G_{req} ⊗ T)

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

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

6) 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.

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

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

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

10) 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.

11) 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.

5. SIMULATION RESULTS

The proposed Energy Efficient Cluster Based Key Management and Authentication (EECBKMA) technique is evaluated through NS2 [17] 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	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

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.

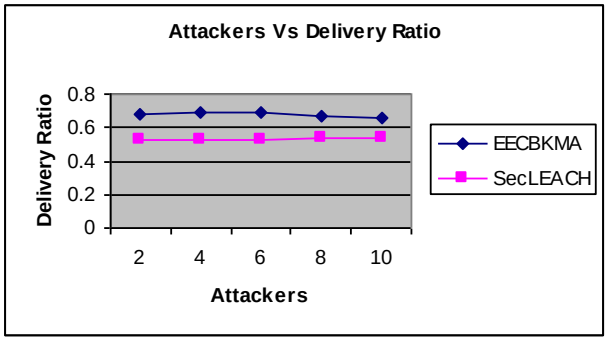

Fig 4: Attackers Vs Delivery Ratio

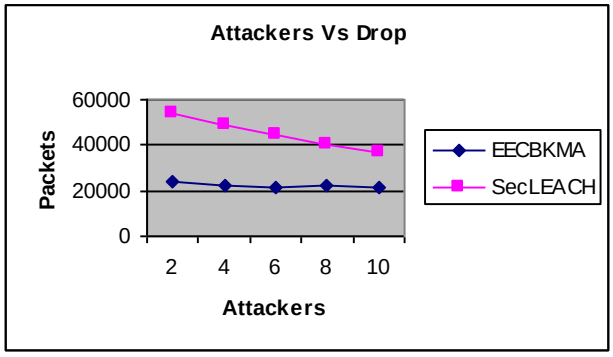

Fig 5: Attackers Vs Drop

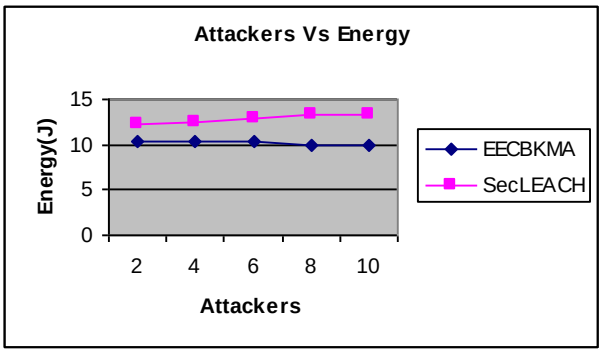

Fig 6: Attackers Vs Energy

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. Figure 4 and 5 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. Figure 6 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.

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.

8. REFERENCES

[1] Yingpeng Sang and Hong Shen "Secure Data Aggregation in Wireless Sensor Networks: A Survey", PDCAT 2006.

[2] 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.

[3] 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.

[4] 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