A KEY RE-DISTRIBUTION AND AUTHENTICATION BASED TECHNIQUE FOR SECURED COMMUNICATION IN CLUSTERED WIRELESS SENSOR NETWORKS WITH NODE MOBILITY

Saswati Mukherjee[1], Matangini Chattopadhyay[1], Samiran Chattopadhyay[2], Amrita Saha[2]

[1]School of Education Technology, Jadavpur University, Kolkata, India – 700 032
sash_cal@rediffmail.com
[2]Deaprtment of Information Technology, Jadavpur University, Kolkata, India – 700 098
samiranc@it.jusl.ac.in

ABSTRACT

Due to application of WSN in mission critical areas, secured message communication is very important. We have attempted to present a methodology that ensures secured communication among nodes in a hierarchical Cluster Based WSN. Our scheme works when member sensor nodes move from one Cluster Head (CH) to another. The proposed scheme is based on Key Re-distribution during node mobility and development of an Authentication Model to check whether the new node in a cluster is an intruder. We have carried out extensive simulation experiments, which demonstrate the efficacy of the proposed scheme. The experiments suggest that the number of message transmission in creases linearly with the number of mobile nodes during key-redistribution when a node moves from one CH to another. We have seen that the detection efficiency of the Authentication Model is 0.9 to 1 when tunable threshold value is 0.02 and sensor nodes are sufficiently mobile.

KEYWORDS

Wireless sensor network, key distribution, isolation table and mobile nodes, intrusion detection.

1. INTRODUCTION

In recent years, Wireless Sensor Networks (WSN) has become an active area of research. Applications of WSN include military sensing, disaster response, health care and intelligent house control etc [2]. WSN involves the deployment of hundreds of low cost, micro-hardware and resource-limited sensor nodes. These sensor nodes are used to sense important data such as temperature, pressure etc. After sensor nodes are deployed, they get self-organized and establish routes automatically. In many typical scenarios, sensor nodes are also connected to the Base Station (BS). Each sensor node carries a limited, generally irreplaceable energy source. Therefore, energy conservation becomes one of the most important performance considerations to extend network lifetime.

Heinzelman et al. [5] proposed a cluster-based WSN (CWSN), a kind of hierarchical WSN that extends network coverage and increases lifetime. After deployment, a set of Cluster Heads (CHs) are selected out of a CWSN. The CHs become the centre of a cluster and the other sensor nodes in this cluster become member nodes. The Member Nodes (MNs) deliver sensed data to the BS through their Cluster Head. Some times the Cluster Heads are more capable in terms of

DOI : 10.5121/ijcnc.2010.2608

resources and may even be tamper resistant. The Member nodes have less resource and are risk-prone. We have used this hierarchical architecture in our paper.

Due to application of WSN in mission critical areas, secured message communication is very important [13]. Public key based asymmetric cryptographic algorithms are shown to be unsuitable for large WSNs. Symmetric key approach is found to be an appropriate cryptography for WSNs due to its low energy consumption and simple hardware needs.

Recent research shows that pre-loading symmetric keys into sensors before they are deployed is a practical method to deal with the key distribution and management problem in wireless sensor networking environment [8]. After the deployment, if two neighboring nodes have some common keys, they can set up a secure link by the shared keys. Two straightforward strategies exist to pre-load symmetric keys into sensors. The first one is called master-key approach, in which all the sensors are pre-loaded a unique symmetric key in its memory. After the deployment, every two nodes in the network use the same symmetric key to encrypt/decrypt the exchanged data between them. This approach is extremely efficient since there is no communication overhead for key establishment and only one key is required to be stored in sensors, but it cannot provide sufficient security for wireless sensor networks. In master-key approach, even one single node's capture could compromise the entire network, which is unacceptable for large-scale wireless sensor networks. Another method is pair wise-key based approach [14], where sets of symmetric keys are preloaded into each sensor node to make sure any two nodes have a unique key between them. This node's capture cannot compromise the secure communication between non-captured nodes. But this approach is not scalable due to extremely large key storage overhead. For a network composed of n nodes, this approach requires each node stores at least (n -1) keys to ensure any two sensors can establish a secure link. These two straightforward approaches show that practical key pre-distribution schemes must strike a balance between the required security and the key storage overhead.

In this paper, we have attempted to present a methodology that ensures secured communication among nodes in a hierarchical Cluster Based WSN. Our scheme works even when member sensor nodes move from one Cluster Head (CH) to another. The proposed scheme is based on Key Re-distribution during node mobility and development of an Authentication Model to check whether the new node in a cluster is an intruder.

We have utilized IKDM (Improved key distribution mechanism) proposed by [8] as a means of key distribution scheme. Thus, any pair of communicating nodes establishes a unique pair wise key based on polynomial key calculation mechanism [10].

Since we have further assumed that the Member Sensor nodes move from one CH to another CH, it necessitates development of a new scheme for secure communication amongst the communicating parties. We have incorporated the necessary modification to the IKDM to take care of the movement of one member node from one CH to a new CH. We have also proposed a mechanism to detect whether a member node that has recently joined a cluster is an intruder or not. This detection actually confirms that during handoff, the mobile Member Sensor node has not been captured and compromised.

We have carried out rigorous simulation experiments which demonstrate the following key points.

- Message transmission during Key Re-distribution phase increases linearly with increased node movements. Thus, the overhead incurred in this scenario is optimal.
- The node detection efficiency of the Authentication Model reaches almost 100% when a tunable threshold parameter is assumed to be 0.02.

The rest of the paper is organized as follows. Section 2 deals with the related works on key distribution mechanisms and intrusion detection techniques. In Section 3, we discuss the modified key distribution scheme to take care of sensor node mobility. In this section, we have also developed a model for authentication and intrusion detection system [13] to determine whether a mobile sensor node is captured during handoff. Section 4 describes the experiments and simulation results of the proposed scheme. In Section 5, we conclude.

2. Related Work

In this paper, two areas have been combined to formulate a model of secured communication. One is mobility of sensor node from one Cluster Head to another by executing hand-over request message so that new keys are established between the mobile node and new Cluster Head. Then, authentication mechanism is performed by the new Cluster Head when the mobile sensor node comes under it.

2.1 Key Distribution Mechanisms

Key distribution in WSN has been extensively studied in recent years. Eschenauer and Gligor [1] proposed a random key pre-distribution scheme where a large size symmetric key pool P is generated first. In this method, the same key may be used by different pairs of sensors in a network and therefore, even the capture of a single sensor may compromise the communication between non-captured nodes. This problem is defined as network resilience in WSN. To improve network resilience, Chan et al. [2] proposed a ''q-composite'' scheme based on Eschenauer et al.'s work which describes any two nodes need to share at least q (q >= 2) common keys to establish a secure link between them.

In Improved Key Distribution Mechanism (IKDM) [8], the bivariate polynomial key pre-distribution scheme has been introduced. Consider a k-degree bivariate polynomial f(x, y), defined as

$$F(x, y) = \sum_{i,j=0}^{k} a_{ij} x^i y^i \qquad \textbf{(1)}$$

where the coefficients a_{ij} ($0 \leq i, j \leq k$) are randomly chosen from a finite field GF(Q), Q is a prime number that is large enough to accommodate a cryptographic key. The bivariate polynomial above has a symmetric property such that

$$f(x, y) = f(y, x) \qquad \textbf{(2)}$$

Each sensor has a unique id in a network. Before deployment, an offline key distribution server (KDS) first initializes sensors by giving each sensor p a polynomial share $g_p(y)$, which is obtained by evaluating f(x, y) at x = p. In order to setup a pair wise key between sensors p and q, they exchange their node ids first, then node p evaluates f (p, y) at y = q, and node q evaluates its stored polynomial f (q, y) at y = p. Since f (p, q) = f (q, p), sensors p and q can obtain the same value from the two distinct calculations, which can be used as their pair wise communication key. The advantage of the bivariate polynomial key pre-distribution scheme is there is no communication overhead during the pair wise key establishment process.

In key distribution phase, secret keys are pre-loaded into sensors before they are deployed [9, 15]. Two different bi-variate symmetric polynomials are used, one is $f_{CH}(x, y)$ which is used to establish pair wise keys between cluster heads. The other is $f_{CHi}(x, y)$ $(0 \leq i \leq m)$ which is used by cluster head CH_i to calculate a secret share for an intended sensor node i. To authenticate and secure the communication between sink node and other nodes in its memory, each key is shared with a particular sensor node or cluster head. Shared pair wise key between cluster head CH_i and sink node is termed as $\mathbf{K_{CHi\text{-}BS}}$, $(1 \le i \le m)$. Pair wise key between sensor S_i and sink node is termed as $\mathbf{K_{Si\text{-}BS}}$, $(1 \le i \le n)$ Each cluster head CH_i stores a symmetric key $K_{CHi\text{-}BS}$, and two polynomial shares $g_{CH}(y)$ and $g_{CHi}(y)$ in its memory, the first is used to assure authentication and secure communication with the sink node and the second is by putting $x=CH_i$ in the two polynomial shares. Only two keys are pre-loaded in each sensor node to reduce the key storage overhead. One is for secure communication with the sink node, randomly initialized by the KDS and the second is for communication with the physical cluster head.

2.2 Intrusion Detection System

The classic intrusion detection approach [12] in wireless environment is tolerant of the compromised nodes within a threshold in a local cluster. This approach is useful to detect intrusion and to revoke compromised nodes. This technique is also energy saving. There are three generic types of packet forwarding misbehaviors: ii) packet dropping, ii) packet duplicating and iii) packet jamming. Packet dropping means that a node drops the packets which it is supposed to forward. Packet duplicating means that a node duplicates the packets which it has already forwarded. When a node consumes significant portion of bandwidth by sending bulk packets, it is called packet jamming.

Zhang and Lee [4] have also studied the problem of intrusion detection in wireless ad-hoc networks. Developing IDS for WSN is based on analysis of local data. There are three main techniques that an intrusion detection system can classify actions; misuse detection, anomaly detection and specification-based detection [4]. In misuse detection or signature-based detection systems, the observed behavior is compared with known attack patterns (signatures). Action patterns that may pose a security threat must be defined and stored to the system. Then, the misuse detection system tries to recognize any "bad" behavior according to these patterns. Anomaly detection systems [11] focus on normal behaviors, rather than attack behaviors. First these systems describe what constitutes a "normal" behavior (usually established by automated training) and then flag any activities that differ from this behavior by a statistically significant amount as intrusion attempts. Specification based detection systems are based on deviations from normal behavior in order to detect attacks, but they are based on manually defined specifications that describe what a correct operation is and monitor any behavior with respect to these constraints.

According to specification based approach [3], rules are defined which map behaviors to normal or abnormal. These specifications for detecting black hole and selective forwarding attacks [15] can be a rule on the number of messages being dropped by a node. The whole network is grouped into clusters which can be partially overlapping. Cluster head is in charge of taking decisions that nodes sending and receiving packets in their cluster are legitimate or not. Watch dogs count the packets in a given time window and calculate the probability of being attacked. In case of an attack, the packets will be dropped at a higher probability than they normally do. If packet drop rate is more than a threshold value then an alarm is generated. Therefore each watch dog node is required to keep track of the packets not being forwarded within a fixed amount of time. Each of the watch dog nodes will apply such rules to produce an intrusion alert.

In this paper, we have used the concepts of [3, 4, 6,] for authentication.

3. HANDLING NODE MOBILITY THROUGH KEY RE-DISTRIBUTION AND AUTHENTICATION MODEL

3.1 Network Model

Typically, a wireless sensor network is composed of a large number of sensor nodes; each sensor node is a small, inexpensive wireless device with limited battery power, memory storage, data processing capacity and short radio transmission range. A number of wireless sensor nodes can be organized into clusters. Each cluster has a cluster head node **(CH)** having more resources in terms of high power batteries, large memory storages, powerful antenna and data processing capacities than sensors. Cluster heads can communicate with each other directly and relay data between its cluster members and the sink node (base station).**Sink node/Base station (BS)** is the most powerful node in a wireless sensor network, it has virtually unlimited computational and communication power, unlimited memory storage capacity, and very large radio transmission range which can reach all the nodes in a network. A large number of wireless sensors are randomly distributed in an area. After deployment, cluster heads (CHs) partition a network into several distinct clusters by some existing clustering algorithms [7, 9]. In our work we have assumed that the low-end sensor nodes in each cluster have the ability to move from one cluster head to another.

3.1 Key Re-Distribution Strategy

We have considered the mobility of the sensor nodes changing their location even after being deployed. In this paper, we have modified the key establishment procedure [8] between a sensor node and a cluster head in the particular case when the sensor node moves to a new cluster head. We have also shown that the communication remains secure even after the modified key establishment procedure is performed to take care of mobility of sensor nodes. The modified key establishment procedure among the mobile sensor node, the old cluster head and the new cluster head is outlined in the following.

Step 1. Sensor node (S_i) while shifting its location from one Cluster Head (CHa) to another cluster head (CHb) sends a hand over request message to the new Cluster Head.
Step 2. The new Cluster Head sends a message to the Base Station (BS) conveying the information that (S_i) is shifting its location from CHa to CHb.
Step 3. The BS picks the ids of two new random cluster heads, say, CHc, CHd. and sends these two ids to the sensor node Si. The sensor node Si substitutes f_{CHa} with f_{CHc} and f_{CHb} with f_{CHd} and obtained k1= f_{CHc}(CHc, y)at (x=CHc, y =Si). and k2=f_{CHd}(CHd, y)at (x=CHd, y =Si) respectively.
Step 4: The sensor node Si then sends the ids of CHc and CHd to its newly joined Cluster Head CHb.
Step 5: The Cluster Head CHb sends the id of mobile sensor node (Si) to CHc and CHd to request the corresponding key shares.
Step 6: Once receives the request message, Cluster Head CHc evaluates its stored polynomial f_{CHc}(CHc, Si) to get the key k1.Similarly Cluster Head CHd evaluates its stored polynomial f_{CHd}(CHd, Si) to get the key k2.
Step 7: After evaluation, Cluster Heads CHc and CHd send these two keys k1 and k2 respectively to the Cluster Head CHb.

Now the secure communication is established between the Cluster Head CHb and sensor node Si by the pairwise key (KSi-CH) = k1$\oplus$ k2, since both of them holds the same key, k1 and k2.

3.3 Security Analysis of Key Re-Distribution Strategy

In our paper, we have executed the IKDM scheme during network initialization and during every hand over. The polynomial being used by the Cluster head (Ch_a), newly joined Cluster head (CH_b) and sensor node (S_i) is kept secret even after the node moves to a new Cluster head. During handover, property of bi-variate polynomial can guarantee the network's security since from exclusive-or operation between the pair-wise key k1 and k2 , it is difficult to gain information about the degree of polynomial being used by the newly joined cluster head (Ch_b) and sensor node (S_i). Even if all the Cluster heads are compromised, none of the keys preloaded in sensor nodes could be compromised in the network and the coefficients of the selected polynomial still cannot be derived by the adversary.

Only the pair-wise key (between the sensor node and the cluster head) needs to be stored in a sensor node. Thus, the memory overhead remains low in this modified scheme. Our simulation results suggest that the message communication overhead increases linearly with the number of mobile nodes.

3.4 Authentication Model

The procedure for modified key establishment between a mobile sensor node and a new cluster head is based on the assumption that there would not be any attack during the time when a sensor node moves to the new cluster head. This may not be always true. In order to safeguard such attacks, we propose to perform an authentication algorithm during handover of a sensor node on the basis of its behavioral characteristics. In line with [3, 4, 6], we have proposed a solution in which a Cluster Head can infer the purpose of the new mobile node joining its cluster. The authentication procedure makes use of well known techniques in IDS, in which a malicious node attacks a network in many ways such as delay and dropping of packets, data alteration, flooding and jamming [3, 4, 6]. In this paper we have considered that the Cluster Head is behaving as watch dog for detecting the malicious activity of sensor node during relocation. A node being malicious depends on several parameters, which are listed below.

- **Delay & Dropping:** In order to detect delay and dropping of packets, the Cluster head will periodically send echo messages to all the sensor nodes in its cluster, (also to check whether they are alive). The sensor nodes are supposed to send back an acknowledgement to the cluster head. A compromised node is engaged in some other activity thereby introducing some noticeable delay in sending the acknowledgment. Or an attacker intent on randomly dropping packets may drop the echo packet and does not send any reply. Thus, packet delay and packet drop will increase in case of compromised nodes.

- **Data Alteration:** In order to detect, an attacker deliberately introduce false sensing data. The Cluster Head can adopt two types of detection strategies, one called the predictor, based on temporal (proximity) / correlation of data,(i.e. the data sent by a particular node over time should be close to the predicted value) and the other called the estimator, based on spatial proximity / correlation of data. Since our model is a mobile WSN, the temporal model is not suitable. We use the spatial model where there should be a close proximity in the data reported by sensor nodes. For compromised nodes, the sensing data may be genuinely different from the estimated data, because of some abrupt changes.

- **Flooding:** The cluster head detects flooding by receiving the same data from a sensor node more frequently than estimated. In this paper, sleep time (time gap between sending two packets) for each node is considered as one of the parameter for flooding detection. If the sleep time is less than a threshold time gap then it is inferred that flooding has occurred and hence the node is detected as malicious.

The outline of our authentication procedure is presented in the following.

- Each Cluster Heads maintains an isolation table storing the count of four parameters influenced by attacks. Each cluster head periodically measures these parameters during the messages transmission by each of the sensor nodes in its cluster in one round.
- If a parameter of a node is found to be crossing threshold, it is noted by the Cluster Head.
- The Cluster Head records the number of rounds in which a given node has been found to be suspicious out of the total number of rounds of such periodic detection between two successive handovers done by that node.
- The sensor node is then tagged as "compromised" if the fraction of times it has been detected suspicious exceeds a chosen threshold value.
- The number of such detections is updated periodically and refreshed again during the next handover.

4. Experiments And Discussions

We have simulated the entire WSN in 10,000 square meters. The field is static and deploys 400 sensor nodes for mobile scenario 2000 sensor nodes for authentication mechanism. All these sensors are then grouped under 40 and 200 cluster heads respectively. The experiments are based on mobile nodes and authentication methods for sensor nodes by the cluster heads.

4.1 Results & Interpretations of Mobility of sensor nodes

Figure 1 shows the relationship between the percentage of mobile nodes and the number of message transmission. The number of sensor nodes is 400 and the simulation time is 4 minutes. It is observed that if we increase the percentage of mobile nodes then the number of message transmission increases linearly.

In Figure 2, we have captured the relationship between the number of random movements and the number of message transmissions. As a matter of fact, the number of nodes considered is 200 and simulation time as 5 minutes. It is observed that message transmission overhead increases linearly with the movement of the nodes. That is, the overhead incurred by the proposed modification is optimal.

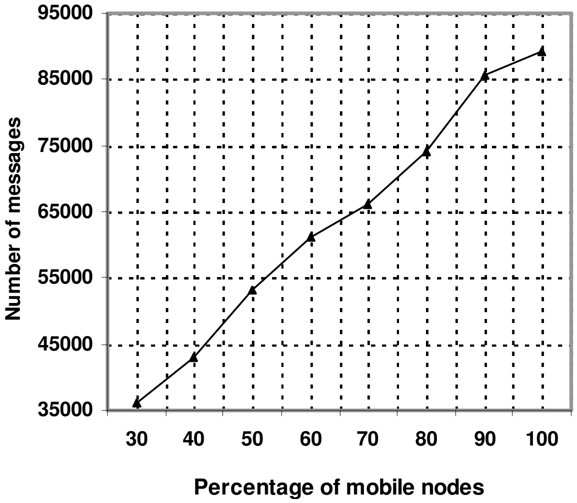

Figure 1:Message transmission versus mobile nodes

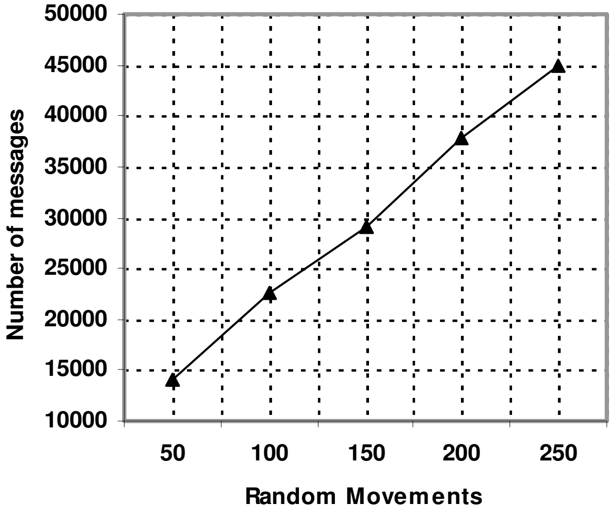

Figure 2: Message Transmission versus random

4.2 Results & Interpretations of Authentication Procedure.

In Figure 3, relationship between the number of sensor nodes and the percentage of compromised mobile nodes detected is captured. Two curves have been plotted with the number of cluster heads as 50 and another as 70.

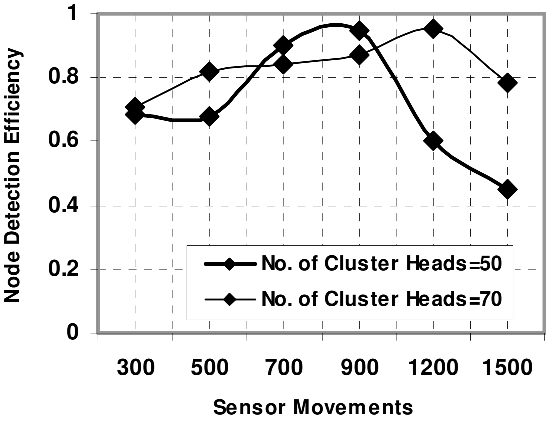

Figure 3: Sensor movements versus node detection efficiency with varying number of Cluster Heads

From Figure 3, we can infer that the detection of compromised mobile nodes reaches almost 100% when the ratio of number of cluster heads to sensor nodes is approximately 7:120.

Figure 4 shows the relationship between the number of sensor node movements and efficiency of detection of malicious nodes. For simulation purpose, we use a random attack model.

Depending on the "degree" of the attack, the attack may be more or less powerful, that is, an attack of higher degree may drop packets or cause delay or alter data more frequently or flood the network more. For example while sending 10 packets, if 8 packets are dropped then degree of attack considered is 4. On the other hand, if 2 packets are dropped then degree of attack considered is 1. From Figure 4, we have observed that varying the degree of attack in the range from 0 to 4, the efficiency of malicious node detection remains more or less constant at 0.9 even with the increased number of sensor movements.

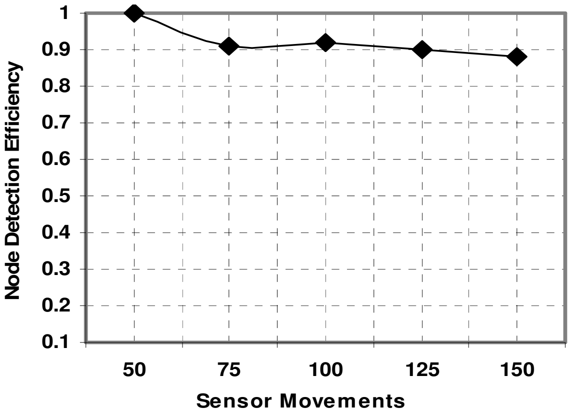

Figure 4: Node detection with random degree of attack efficiency with varying number of Cluster Heads

In Figure 5, the relationship between the number of sensor movements and efficient detection of correct nodes has been depicted considering sensor nodes as 200, percentage of attack as 20%, threshold value as 0.02. From Figure 5, we can conclude that the node detection efficiency increases and eventually becomes constant at 100 percent, as the number of sensor movements increases with degree of attack as 4.

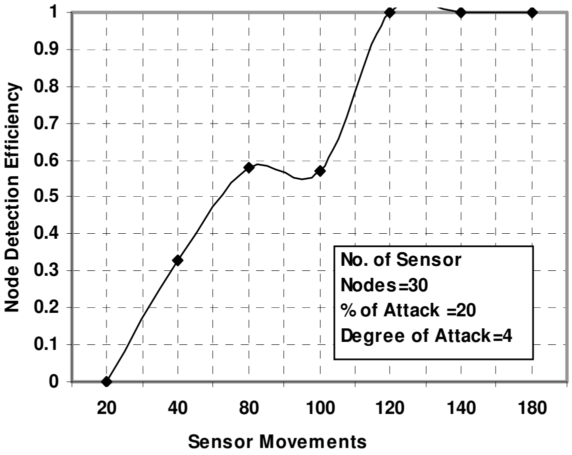

Figure 5: Node detection with degree of attack as 4

Figure 6 shows the relationship between different threshold values and compromised node detection efficiency. For simulation purpose, sensor nodes considered is 100, number of movements as 180, percentage of attack is 20 and simulation time as 180 seconds. From figure 6, we can infer that when degree of attack is random, malicious node detection efficiency is approximately 0.78 at threshold value 0.14. Similarly when degree of attack is 4, node detection is almost 0.6 with threshold values as 4. It has been observed that the correct detection of attacked nodes gains maximum efficiency at a threshold value of 0.02.

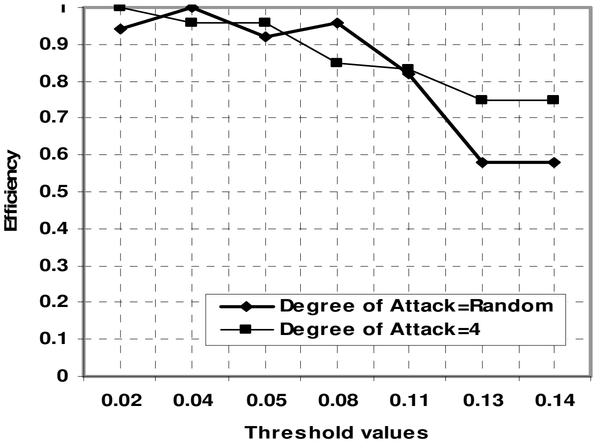

Figure 6: Treshold value versus node detection efficiency

4.3 Communication & Computational Overhead Analysis

The communication overhead incurred at the sensor nodes is due to sending the acknowledgements of the echo message sent periodically by the cluster head. The overhead incurred in this stage is very nominal. The Cluster head periodically broadcast echo packets, count and update the behavioral history table for each of the sensors currently in its cluster. All these procedures involve some computation. Each cluster head perform intrusion detection process during handover thereby needs some storage to store the dynamic table of behavioral characteristics for each of the nodes under it. But since a cluster head is employed with greater computational and storage capabilities, such overhead can be practically handled.

5. CONCLUSION

We have considered the problem of secured communication in a cluster based WSN even when the sensor nodes may move from one cluster head (CH) to another. We have modified an existing polynomial based key distribution strategy to ensure an appropriate key re-distribution at the time of hand-off when a sensor node moves from one cluster head to another. This re-distribution mechanism assumes that during hand-off the mobile node is not going to be compromised. We have further explored the possibility of authenticating the mobile node at the time when it joins the cluster of a new cluster head. The proposed authentication model uses behavioral analysis as is common for an intrusion detection system. The new cluster head acts as a watch dog and monitors the newly joined node for malicious behavior such as delay and drop, flooding etc..

We have carried out extensive simulation experiments, which demonstrate the efficacy of the proposed scheme. We have seen that the number of message transmission during key-redistribution when a node moves from one CH to another increases linearly with the number of mobile nodes. This observation implies that the overhead for incorporating mobility is as expected. It is also observed that the efficiency of the proposed authentication model becomes the maximum for an appropriate ratio of cluster heads and mobile nodes. We have also seen that the efficiency of the authentication model is very high even when the number of attacks is large and the efficiency remains high after the number of node movements crosses a threshold. We have seen that the detection efficiency of the Authentication Model is 0.9 to 1 when the threshold parameter is 0.02 and sensor nodes are sufficiently mobile.

In the future, we would like to study the proposed system by incorporating formal attacks models and by having different mobility patterns. We would also like to extend the study to multi-hop hierarchical Wireless Sensor Networks.

REFERENCES

[1] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, November 2002.

[2] H. Chan, A. Perrig, D. Song, Random key pre-distribution schemes for sensor networks, in: Proceedings of IEEE Symposium on Security and Privacy, Berkeley, California, May 11–14 2003, pp. 197–213.

[3] Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari, Kumar Sidharth Choudhary, “Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information”, Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009.

[4] Y.Zhang and W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks”, Proc. of ACM MobiCom, pp. 275-283, 2000.

[5] Heinzelman, W. B., Chandrakasan, A. P., and Balakrishnan, H. 2002. An Application-Specific Protocol Architecture for Wireless Microsensor Networks. IEEE Transactions on Wireless Networking, Vol. 1, Issue. 4, pp. 660-670.

[6] Chien-Chung Su, Ko-Ming Chang, Yau-Hwang Kuo, Mong-Fong Horng “The New Intrusion Prevention and Detection Approaches for Clustering-based Sensor Networks”, IEEE Communications Society, 2005

[7] S.Madhavi, “An Intrusion Detection System In Mobile Adhoc Networks”, Proceedings of the International Conference on Information Security and Assurance, 2008.

[8] Yi Cheng, Dharma P. Agrawal, An improved key distribution mechanism for large-scale hierarchical wireless sensor networks, Proceedings in Science Direct, May 2007, pp. 35-48.

[9] D. Liu, P. Ning, Location-based pairwise key establishments for relatively static sensor networks, in: Proceedings of 2003 ACM Workshop on Security of Ad hoc and Sensor Networks (SASN’03), October 31, 2003. George W. Johnson Center at George Mason University, Fairfax, VA, USA.

[10] R. Blom, An optimal class of symmetric key generation systems, in: Thomas Beth, Norbert Cot, Ingemar Ingemarsson (Eds.), Advances in Cryptology: Proceedings of EUROCRYPT 84, Lecture Notes in Computer Science, vol. 209, pp. 335–338.

[11] Qinghua Wang, Tingting Zhang, “Detecting Anomaly Node Behavior in Wireless Sensor Networks”, 21st International Conference on Advanced Information Networking and Applications Workshops, IEEE, 2007.

[12] Leon Reznik, Bakytzhan K. Bitemirov, Michael Negnevitsky, “Intrusion Detection in Sensor Networks Based on Measurements”, Conference on IEEE sensors, 2009.

[13] Farooq Anjum, Petros Mouchtaris, “Security for Wireless Ad--hoc Networks”, Security for Wireless Ad--hoc Networks, John Wiley & Sons, November 2006.

[14] W. Du, J. Deng, Y.S. Han, P.K. Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, in: Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27–31, 2003, pp. 42–51.

[15] Zaw Tun and Aung Htein Maw, “Wormhole Attack Detection in Wireless Sensor Networks”, World Academy of Science, Engineering and Technology, 2008.

Authors' Information

Saswati Mukherjee received her M.E. degree (Multimedia Development) from Jadavpur University in 2006. Currently, she is a lecturer in the School of Education Technology, Jadavpur University and pursuing her research work in Jadavpur University. Her main research interests are security of wireless ad hoc and sensor networks and game theory.

Matangini Chattopadhyay obtained her Bachelor of Engineering degree in Electrical Engineering from Bengal Engineering College, Shibpur, India. She received her Masters and Ph.D. degrees from Jadavpur University. She is an associate Professor in the School of Education Technology, Jadavpur University. Her research interests include middleware for wireless and mobile computers, security in wireless networks, and game theory.

Samiran Chattopadhyay received his Bachelor of Technology (B.Tech) degree in Computer Science and Engineering from IIT Kharagpur in 1987. He received his M.Tech. degree from the same department in 1989 and received his Ph.D Degree from Jadavpur University in 1993. Presently, he is a professor in the department of Information Technology, Jadavpur University, India. He has been associated with many leading organizations like Motorola, NEC Laboratory, Computer Associates, Agilent and Interra Systems India Pvt. Ltd. Author of over 50 papers in journals and conferences, his research interests span wireless and mobile communication, game theory, and computational geometry.

Amrita Saha has completed her B.E degree in Information Technology in the Jadavpur University. She is pursuing higher studies at I.I.T Mumbai, India.