ISSN:2231-0711
www.ijcset.net

An Active En-route Filtering Scheme for Secured Data Dissemination in Wireless Sensor Networks

N.Parashuram, Y.Sanjay sai raj, A.Sagar, B.Uma

IT Department, G.Pullaiah College of Engineering & technology
Kurnool, Andhra Pradesh, India

***Abstract*-In wireless sensor networks, oppugneries can inject false data reports via compromised nodes and launch Denial of Service attacks against legitimate reports. Recently, a number of filtering schemes against false reports have been proposed. However, they either lack strong filtering capacity or cannot support highly dynamic sensor networks very well. Moreover, few of them can deal with Denial of Service (DoS) attacks simultaneously. Wireless Sensor networks are deprived of high memory requirements, high processing power, and are limited in usage of efficient security mechanisms. They are susceptible to possible node compromise, passive and active attacks. Most of the public key cryptographic techniques are found to be more work prone with the secure exchange of keys, lengthy hash operations with high processing rounds etc. Even though comprehensive surveys are made in disseminating sensor reports securely to the sink, those mechanisms do not provide adequate verification process of reports from source to destination nor do they completely mitigate false report injection attacks and Denial of Service attacks (DoS). Moreover these mechanisms concentrate on hop-by-hop security paradigms leaving end-to-end security at high risk. In this paper we propose a dynamic en-route filtering scheme that addresses security mechanism for data dissemination in wireless sensor networks. In our scheme, each node has a hash chain of authentication keys used to endorse reports, The proposed work aims at decreasing the attackers malicious intent and activity compared to the existing mechanisms by the responsibility being taken by the cluster heads in finding the attackers within the clusters and marking them as malicious and later intimating to the base station. The legitimacy of the report being forwarded by the cluster head is collectively endorsed by Message authentication codes. We evaluate our mechanism through extensive analysis of relocating the position of malicious nodes in the event area and thereby analyzing its performance through secured data dissemination.**

Keywords-*Dos Attacks, Wireless Sensor Networks, False Data Reports, Message Authentication Endorse Reports.*

1 INTRODUCTION

Wireless sensor networks consist of the large number of a small sensor nodes having limited computation capacity, restricted memory space, limited power resource, and short range radio communication device. In military applications, sensor nodes may deployed in hostile environments such as battlefields to monitor the activities of enemy forces. In these scenarios, sensor networks may suffer different types of malicious attacks. One type is called false report injection attacks **[1]**, in which adversaries inject into sensor networks the false data reports containing nonexistent events or faked readings from compromised nodes.

These attacks not only cause false alarms at the base station, but also drain out the limited energy of forwarding nodes. Since they operate on battery power **[2]**, they cannot able to have high and long distant packet transmissions, sufficient memory capacity, high processing capacity and energy for prolonged functioning. When deployed in unattended terrains for critical military applications they have to configuration, themselves and must make use of the power efficiently to have an extended operating life time.

Most of the battery's energy is consumed for communication and this is the reason why sensor nodes enter into sleep mode when they are idle. In addition to this, the rates of transmissions are expected to be minimal, because an adversary in a terrain can monitor the wireless spectrum to interpret the critical data being sent. He may even try to impersonate the data if it is sent without using any security mechanism or he may try to modify the content of the report there by, trying to forge an incident which has not happened at all. Thus causing severe problems related to confidentiality, integrity and availabilities. Surveys made up to date reveals the presence of different types of attacks in WSN which could lead to serious availability, confidentiality and authenticity problems of the reports. WSN finds its application widely in military, environmental, healthcares, productions etc. Some specific applications are Detection of biological agents, hazardous chemicals, Forest fire detection, rush hour traffic monitoring, product quality monitoring, managing inventory etc. Such mission critical applications emphasized the need for research in the field of security in sensor networks. Due to increase in the application of WSN in various fields, the problems threatening to its security also proportionally increased day by day.

2 RELATED WORK

We first discuss existing filtering schemes, then introduce some routing protocols used in wireless sensor networks. The routing strategies of these protocols affect the way that sensor nodes can exchange and disseminate key information, so they have significant impact on filtering schemes.

Ye et. al. proposed Statistical En-route filtering **[3]** Scheme which requires each report to be endorsed by multiple sensor nodes by encrypting the report with their random pre-distributed keys. This scheme functions on the mechanism of

checking the keys of intermediate nodes with the encrypted report received on its way to the base station. If the keys are matched as the result of checking process, the reports are considered to be authenticated. This type of mechanism relies on probabilistic key sharing in which only a part of the illegitimate reports are detected and dropped. Zhu et al. **[1]** proposed an Interleaved Hop-by-hop Authentication to detect false reports. This scheme requires pre-route interleaved associations maintained between sensor nodes to share the sensor secrets between upper associated nodes and lower associated nodes. Due to the unpredictable nature of the wireless medium, it is not possible for a large sensor network to have determined routing paths consistently and the association too requires global knowledge of the network which is considered as tedious task.

A public key based approach **[4]** proposed by Zhang et.al. found to provide good security resilience but still it is a bilinear pairing scheme which is too expensive to be afforded by a low power sensor hardware. Kui Ren et al. proposed Providing Location aware End to end Data Security which utilizes location ased information as keys to encrypt the reports. This scheme addresses data availability requirement in addition to false report filtering and uses the concept of virtual geographic grid to partition the targeted terrain to obtain the location information to be used in its keys. They use three different types of keys to encrypt the report which incurs additional overhead than the existing mechanisms and also computing location based information immediately after the sensor node deployment is a time consuming process which results in report reception delay in the network which affect data availability requirement.

Although dynamic keying techniques are more attack resilient than static ones, a significant disadvantage is that they increase the communication overhead due to keys being refreshed or redistributed from time to time in the network. There are a lot of reasons for key refreshing which includes updating keys after revocation, refreshment of keys to avoid them from becoming stale, or due to dynamic changes in the network topology **[5]**.

2.1 Routing Protocols of Sensor Networks

Several distributed distance-vector based routing protocols **[6]** have been designed and implemented in TinyOS. In these protocols, each node periodically broadcasts its routing cost to the sink, e.g., the base station, and builds a routing table according to the information received from its neighbors. Route is selected based on the routing metrics such as hop count or link quality.

3 SECURITY MODEL

We consider a large sensor network field where nodes are deployed. So after the network initialization phase the sensor nodes forms into groups and elect a cluster head based on different parameters like remaining energy etc. Whenever events of interest occurs in the terrain say if a tank moves, all the cluster members near to the event will sense the happening and report to their cluster heads. On receiving the reports cluster head aggregates them and sends a single copy of the valid report to the base station through selected report forwarding nodes. The selections of report forwarding nodes are up to the underlying routing protocol's work . And also the selection parameters are independent of the application. We assume that there are attackers present within the terrain are capable of monitoring the communication pattern between the sensor members and the cluster head to guess the message from the reports if intercepted. We assume that each cluster contains at most t-1 compromised nodes, which may collaborate with each other to generate false reports by sharing their secret key information. The potential attacks which we consider in our work DoS attacks **[7]**. DoS attacks include selective forwarding and report disruption.

3.1 DoS attacks

Under this attack a malicious node can actively insert itself in the mid of the report forwarding route and can selectively drop reports of its interest which is called as selective forwarding attack **[7]** and through inserting an invalid authentication information to the reports, an attacker can make a legitimate cluster to drop the reports which is called as report disruption attack. The compromised nodes can prevent the legitimatereports from being delivered to the base station, by either selectively dropping some reports, (which are called the *selective forwarding attacks*) or intentionally inserting invalid authentication information into the reports to make them filtered by other forwarding nodes(which are called the *report disruption attacks*).

4 OUR CONSTRUCTION

In this paper, we propose Secured Data Dissemination with the help of nested MAC structures that provides additional data confidentiality strength, attacker detection and elimination from the report forwarding path and strong filtering capacity which also ensures end to end data security of the reports delivered to the base station. The proposed scheme makes use of nested MAC structures in handling the authentication keys of each node participating in the reporting process. The number of authentication key checking process is limited to the number equivalent to the number of cluster members of cluster head. In the proposed scheme control messages are used to disseminate and disclose the keys to forwarding sensor nodes and later allow the same to verify the keys by decrypting them and finding a shared secret key. To accomplish this every sensor node maintains 2 secret key pools and a seed key. A series of authentication keys can be derived from this seed key when there is a need. Hence when a shared secret key is found its corresponding authentication keys are derived and stored in the memory of sensor nodes. Thus the keys selected randomly from the key pools are used to encrypt the authentication keys which are collectively used for producing MAC of the report and later used for the reports collective endorsement.

A. Assumptions

The sensor nodes are densely deployed in unattended terrains. So prior to the network deployment each node is preloaded with a seed key and two secret key pools called l and z. The communication region of WSN is modeled as a circle of radius r, which is nothing but the transmission range. We also consider only bidirectional links between neighbor nodes. Hence all sort of communication between the neighbors can be done only if they are within the radius r. Out of a cluster a cluster head is selected and the role of a cluster head is transferable to balance the energy consumption. A cluster head performs the same function of sensing as that of a normal cluster member and hence do not have any differentiation. We also assume that the topology of the WSN is highly dynamic and can frequently change because of mobility and switching of the states between active and sleeping modes.

B. Phases of Secured Data Dissemination

The whole of secured data dissemination from the cluster head to the base station is achieved in four phases. They are i) Key pre-distribution, ii) Cluster Head Verification iii) Key Dissemination, iv) Verification and Report Forwarding. In Key pre-distribution phase the necessary key materials needed for the secure communication is loaded prior to the deployment.

In Cluster Head verification phase the verification of the nested HMAC ed report are done. In Key Dissemination phase, the authentication keys derived and collected are disseminated

to the report forwarding nodes. In Report forwarding phase, verification of the reports are performed in the report forwarding nodes and final delivery to the base station is achieved.

C. Key Pre-Distribution

Under key pre-distribution phase every sensor node before to the deployment in the terrain are loaded with a seed key. From the seed key, sequence of pre-authentication keys can be formed using a common hashing function such as MD5 in our work. Let m denote the length of the hash chain formed. Given node vi as well its seed key $k_m^{v_i}$ its pre-authentication keys can be calculated as follows:

$$k_{m-1}^{v_i} = h(k_m^{v_i}$$

$$k_{m-2}^{v_i} = h\left(k_{m-1}^{v_i}\right) = h^2(k_m^{v_i}$$

.

$$k_1^{v_i} = h^{m-1}(k_m^{v_i}$$

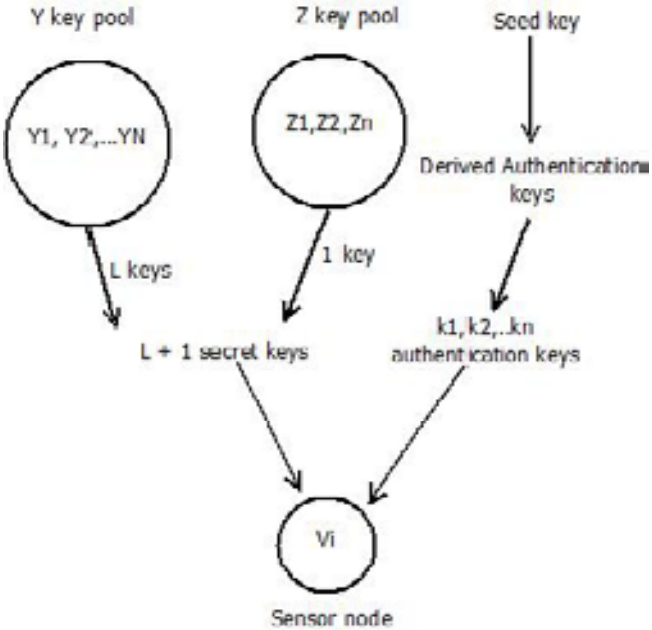

Fig. 1: Secret Key structures

4.1 Cluster Head Verification

Pre-authentication keys derived from the seed key are encrypted using l + 1 secret keys and are used for producing Nested HMAC of the report. Thus the notations used for producing Nested HMAC are as follows.

H= embedded hash function (MD5).

IV= initialization vector or initial value input to hash function.

M = message (event sensed) input to HMAC (including the padding specified in the embedded hash function)

NEHF= length of hash code produced by embedded hash function (MD5).

KAUTH= authentication key as a result of encryption of preauthentication key and secret keys.

K^+= KAUTH padded with zeros on the left so that the result is equal to number of bits in the message block.

Then the Nested HMAC'ed report can be expressed as below.

$$HMAC_{K_{AUTH}} = H[(K^+ \oplus opad)||$$
$$H[(K^+ \oplus ipad)||M]]|$$

Thus the Nested HMAC along with the report is sent by the cluster members to their cluster heads. Before the reports are forwarded to the report forwarding nodes cluster head is responsible for collecting all the authentication keys (K_{AUTH}) and pack them in a control message $K_{(n)}$ and send to selected report forward nodes. Since the cluster head knew authentication keys of all the members, it produces Nested MAC of some reports received from the cluster members. It now checks the received Nested HMAC with the computed Nested HMAC. Upon successful verification it sends the reports in determined rounds to the report forwarding nodes.

The authentication keys K_{AUTH} can be produced as follows. Each node constructs authentication key, which contains L+1copies of pre-authentication keys, each encrypted using a different one of its secret keys.

4.1.1 Key Dissemination

The authentication keys collected from the cluster heads are packed into a control message called K (n) and the format of K_{AUTH} is

$$K_{(n)} = K_{AUTH_{v_1}}, \ldots, K_{AUTH_{v_n}}$$

Keys are forwarded to q report forwarding nodes to enhance verification process of the Nested MAC'ed reports. After the keys are disseminated to q report forwarding nodes, the cluster head collects all first authentication keys of the cluster members and pack them in a control message called K (t) and send them to report forwarding nodes. However, this method is vulnerable to attackers, i.e., an attacker can pretend to be a legitimate cluster head and inject arbitrary reports followed by falsified authentication keys. By disclosing K (t), forwarding nodes can verify the authenticity of the disclosed keys which are in turn used for checking the validity and integrity of the sensor reports. The format of K (t) is

$$K(t) = \{ K_{AUTH_{v_{i_1}}}, \ldots, K_{AUTH_{v_{i_t}}} \}$$

4.1.2 Verification and Report Forwarding

When a report forwarding node receives K (n), it performs the following operations. It verifies K (n) to see whether it contains at least t distinct indexes of z-keys. It actually receives a Nested HMAC and a raw report in addition. It first produces HMAC of the raw report and verifies it with the received Nested HMAC. If the computed and received Nested HMACs are same it verifies the distinct indexes of z-key. If these two conditions are failed then this K (n) is assumed to be a forged one from the attacker and should be dropped. And obviously the report also is dropped. t checks for a shared key of same index in K (n). So when a shared key is found its corresponding authentication key can be decrypted using that key. Hence this process assures that the decryption key is the correct one by checking the index encrypted along with the authentication key. If not it discards K (n). K (n) is disseminated till the base station because if any attacker compromises the last node before base station, it can launch the fore said attacks and can ruin the whole critical report causing a great loss to all the sensor nodes computation power and energy. Each node on receiving the report does the above said process and delivers the reports to the base station successfully.

4.1.3 Proposed Algorithm

The overall process of Secured Dissemination which involves four phases as shown in fig. 2 is explained in the form of Algorithms 1 and 2.

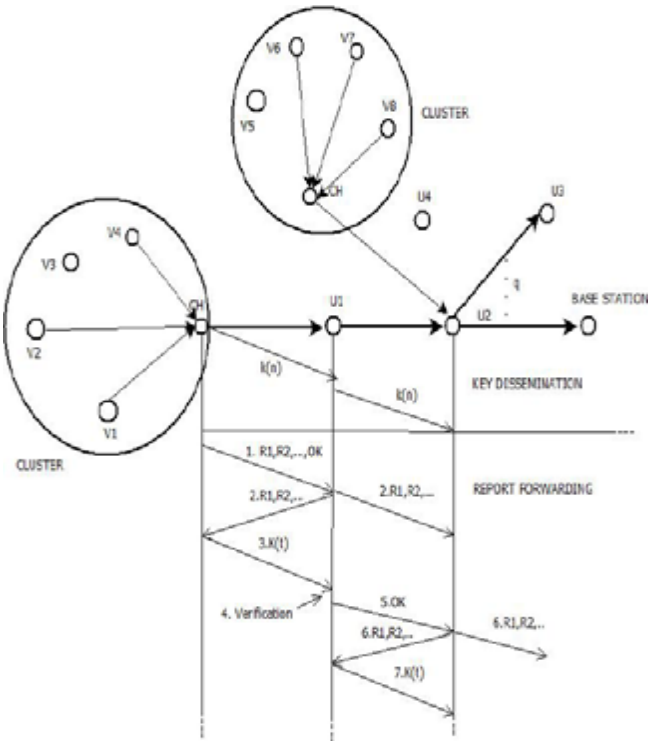

Fig. 2: Overall Process of Key Distribution and Report Forwarding

Algorithm 1 Cluster Head

1: For i=1 to l do
2: Collect r[i] + M from n[i]
3: //Produce Nested HMAC [M]
4: HMACKAUTH=H[(K+ ⊕ opad) + H[(K+ ⊕ ipad) + M]]
5: Compare computed HMAC with Produced HMAC.
6: If HMACKAUTH is valid
7: //Aggregate the report.
8: Report R=r(vi1),. . . ,r(vin)
9: Discard redundant r[i]
10: End if.
11: End for.
12: //Collect Authentication keys KAUTH from n[i].
13: K(n) = KAUTH(v1) ,. . . ,KAUTH(vn)
14: Select Report Forward Nodes to q.
15: Disseminate K(n) to q
16: Forward R to Uj .
17: Forward OK to Uj .
18: Collect first Authentication keys of cluster members
19: Disseminate K(t) to q.

Algorithm 2 Report Forwarding Nodes
1: For i=1 to l do
2: Receive R from CH
3: Receive OK from CH
4: Forward R to U(j+1).
5: End for
6: // R contains HMAC + M.
7: // Produce Nested HMAC [M]
8: $HMACK_{AUTH}=H[(K^{+} \oplus opad) + H[(K^{+} \oplus ipad) + M]]$
9: Compare computed HMAC with Produced HMAC
10: If HMACKAUTH is valid
11: T = id[z]
12: If (K(n) != t) + (id(K(n))zi == id(K(t))zi)
13: Send OK to Uj+1
14: Else
15: Send "Drop" to Uj+1
16: End if
17: End if

A forwarding node holding a larger index of y-key can always decrypt a sensing nodes authentication key from K(n). After a forwarding node decrypts an authentication key from K(n), it updates K(n) by encrypting the authentication key using its own y-key and then forwards the updated K(n) to its downstream neighbor nodes. By enforcing this substitution at every forwarding node, the indexes of y-keys contained in K(n) will be increased gradually. So it becomes harder and harder for the nodes closer to the base station to decrypt the authentication key from K(n). Hence the proposed algorithm achieves better strength against the decryption of the authentication keys than the existing mechanisms.

5 SIMULATION EVALUATION

We study the performance of our scheme by simulation and compare it with others such as SEF, IHA, and CCEF in terms of filtering capacity, fraction of false reports filtered, and memory requirement in different environments.

A. **Simulation Setup**

- 103 nodes are randomly deployed into a 103 x 103 m2 square field with the base station located at the center. The transmission range of each node is 50 m. These nodes are divided into 100 clusters, where each cluster contains exactly n=10 nodes.
- Each node picks l=2 y-keys and one z-key, where the size of y-key pool and z-key pool is v=w=20.
- The size of memory used by each node is denoted as mem, and measured by the number of keys that each node stores.

Typically, mem=50. In our simulation, each cluster-head disseminates auth-keys to forwarding nodes. One node may need to store the auth-keys from different clusters. It divides its memory into equal-sized slots and assigns one slot to each cluster that it serves.

- Each node forwards K(n) to q=2 selected downstream neighbor nodes, until K(n) reaches the base station or has been forwarded hmax hops. Typically, hmax=10.
- Each aggregated report contains t=5 MACs, and there are at most t-1=4 compromised nodes in each cluster. The compromised nodes from the same cluster collaborate with each other to share the compromised secret keys.
- To simulate the dynamic topology, we apply a simple ON/OFF between each cluster-head and the base station for transmitting control messages in both directions. To make them work on top of GPSR, we revise them accordingly and design a *revised IHA* and a *revised CCEF*. Moreover, in the revised CCEF, we let each forwarding node always keep on forwarding the reports for which it has no witness key. This is different from the original CCEF in which those reports are always discarded.

5.1 Simulation Results

1) Our scheme can better deal with the dynamic topology of sensor networks. It achieves a higher filtering capacity and filters out more false reports than others in dynamic network.
2) *Hill Climbing* increases the filtering capacity of our scheme greatly and balances the memory requirement among sensor nodes.
3). We have used NS-2 **[8]** for the simulation of the proposed scheme. Sensor network packages **[9]** are config.d on the top of NS-2, which involves the configuration of phenomenon channel, data channel, phenomenon nodes with phenomenon routing protocol to capture real time events, phenomenon nodes pulse rate, phenomenon type, sensor nodes, non sensor nodes, sensor agents, UDP agents, sensor applications etc. Nodes are randomly deployed into a terrain of dimension 600m X 600m. The detailed information of the simulation environment is shown in Table1.

Simulation Area - 600 m x 600 m
Number of sensor nodes - 25 to 100
Number of Attacker nodes - 0 to 5
Propagation Model - Two Ray Ground
Interface Queue Size - 5000 packets
Routing Protocol - AODV
Data Rate - 11 Mbps
Packet Size - 1026 bytes
Simulation Time - 100 seconds

Table 1: Simulation Parameters

5.2 Performance Evaluation

With nodes randomly deployed in the terrain, we have introduced malicious attackers to launch a Selective forwarding attack on the Report forwarding nodes and made them to selectively drop the sensor reports from cluster head. Also Report disruption attack is launched which involves dropping of the complete legitimate share of the sensor report by the cluster head due to the single illegitimate HMAC offered by an attacker. Since the nodes are on mobility pattern, the report forwarding nodes may serve for two or more clusters. Hence more amount of critical data is sent

through them. Therefore such type of nodes will be of higher interest to the attackers and they serve as hot spots. We have evaluated our secured data dissemination mechanism in terms of Packet Delivery Ratio, Average Delay, Throughput, Packet loss under these attacked scenarios and in the proposed scheme scenario and found remarkable improvement in their performances.

5.3 Packet Delivery Ratio

Packet Delivery Ratio (PDR) — also known as the ratio of the data packets delivered to the destinations to those generated by the CBR sources **[10]**. The PDR shows how successful a protocol performs delivering packets from source to destination. The higher value gives better results. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness. Scenario has been set up for 25 nodes out of which 5 nodes are config.d to be malicious. When the simulation is started the route discovery process of AODV is done and report forwarding nodes are chosen. Now the environment is ready for the sensor nodes to sense the events and report them to their respective clusters. As the simulation time progresses the malicious nodes activity starts to increase and as a result they drop the packets selectively as in case of selective forwarding attack or completely dropped by cluster head as in case of report disruption attack. Hence Packet delivery ratio is analyzed in different scenarios such as in the presence of intruders, without the presence of intruders and after the simulation of Secured Dissemination mechanism etc. It is observed to have 15 % increase in the Packet Delivery Ratio. after the Enroute mechanism is employed. This is why because when Nested HMAC's are verified by both the cluster head and report forwarding nodes are done it is difficult for an attacker to forge a false event that hasn't happened and to make the cluster head forward that report further to the report forwarding nodes. Hence through Enroute mechanism the false report with invalid HMAC is identified and thereby eliminated before they are forwarded to the report forwarding nodes.

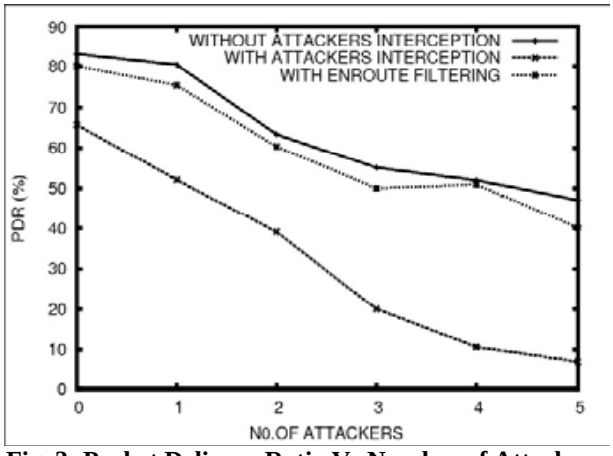

Fig. 3: Packet Delivery Ratio Vs Number of Attackers

5.4 Average End-to-End Delay

There are possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. Average end-to-end delay is an average end-to-end delay of data packets. Once the time difference between every CBR packet sent and received was recorded, dividing the total time difference over the total number of CBR packets received gives the average end-to-end delay for the received packets. This metric describes the packet delivery time: the lower the end-to-end delay the better the application performance. Same scenario is maintained, in which the Average End to End Delay is computed by varying the number of attackers. As shown in the fig. 4 the delay in the Enroute mechanism is found to be comparatively less than that of the normal scenario because when the cluster head finds an intruder in the path it breaks the path by discarding the path where the attacker is present and intimating the same to the base station. Generally reactive protocols like AODV tend to reduce the control traffic messages overhead at the cost of increased latency in finding new routes. But with the proposed Enroute mechanism it is observed to have a decrease of 0.5 seconds in the reception of sensed reports to the base station.

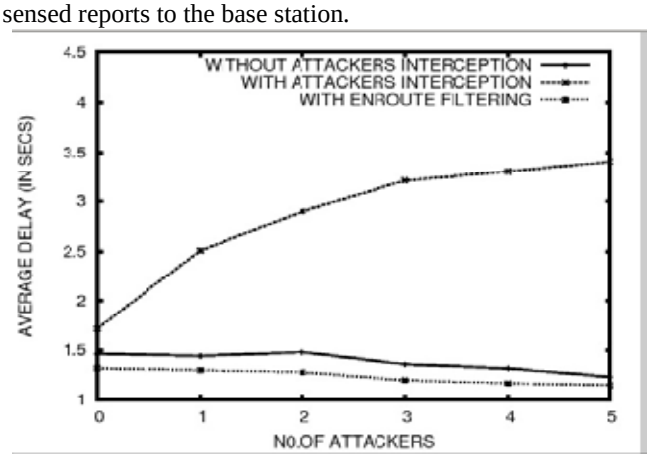

Fig. 4: Average End to End Delay Vs Number of Attackers

5.5 Packet Loss

Mobility-related packet loss may occur at both the network layer and the MAC layer. When a packet arrives at the network layer, the routing protocol forwards the packet if a valid route to the destination is known. Otherwise, the packet is buffered until a route is available. A packet is dropped in two cases: the buffer is full when the packet needs to be buffered and the time that the packet has been buffered exceeds the limit. As observed from the fig. 5, packet loss seems to be very high when there is increase in the attackers count. Attackers try to launch selective forwarding attack, report disruption attack and false report injection attack in which the total availability requirement of the critical information is lost leading to total energy drain of the resource constrained sensor nodes or false positives or false

negatives intimation at the base station. Under this state the malicious node drops all the packets from a selective node or selective packets from a node leading to a huge packet loss in the network. With Enroute Filtering mechanism packet loss is reduced to 40% which is achieved by the identification of attacker nodes through verification and report forwarding phase implemented in the cluster heads.

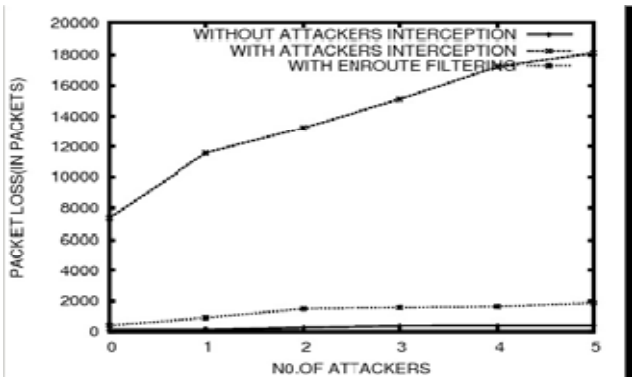

Fig. 5: Packet Loss Vs Number of Attacker nodes

5.6 Throughput

Throughput is defined as the average rate of successful message delivery over a communication channel or sum of the data rates that are delivered to all terminals in a network. As there is heavy packet loss with the presence of malicious activity, the throughput of the network is declined to a percentage of 40. Throughput of the network highly suffers because of DoS attacks and False report injection attacks. False report injection attack degrades the throughput level because, of the single illegitimate HMAC offered to the cluster head there is a great vulnerability of the reports being dropped by a legitimate cluster head. As shown in the fig. 6 Enroute Filtering mechanism achieves a throughput increase of 8% in the presence of attackers.

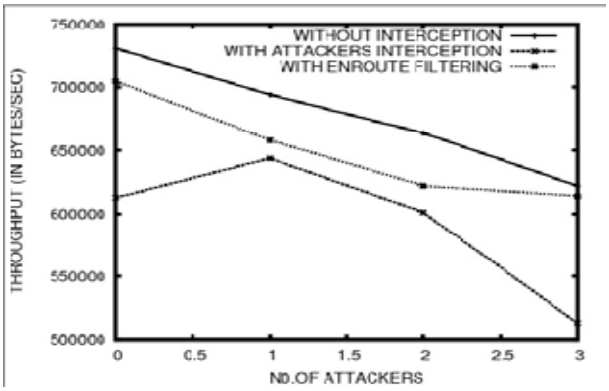

Fig. 6 : Throughput Vs Number of Attacker

DISCUSSION AND EXTENSIONS

In this paper, we propose an active en-route quarantine scheme for filtering false data injection attacks and DoS attacks in wireless sensor networks. In our scheme, each node uses its own auth-keys to authenticate their reports and a legitimate report should be endorsed by nodes. The auth-keys of each node form a hash chain and are updated in each round. The cluster-head disseminates the first auth-key of every node to forwarding nodes and then sends the reports followed by disclosed auth-keys. The forwarding nodes verify the authenticity of the disclosed keys by hashing the disseminated keys and then check the integrity and validity of the reports using the disclosed keys. According to the verification results, theyinform the next-hop nodes to either drop or keep on forwarding the reports. This process is repeated by each forwarding node at every hop. A major challenge for a Wireless Sensor Network lies in the energy constraint at each node, which poses a fundamental limit on the network life time. Even though there are many enroute filtering schemes available in the literature they either lack to support the dynamic nature of the sensor networks or they cannot efficiently mitigate the adversaries' activities.

Hence this en-route filtering scheme is currently an area of much research among the security professionals.

REFERENCES

[1]. S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-Hop authentication scheme for filtering of injected false data in sensor networks," in *Proc. IEEE Symp. Security Privacy*, 2004, pp. 259–271.

[2]. Akyildiz, I. F. Su, W. Sankarasubramaniam, Y. Cayirci, E. (2002), "A Survey on Sensor Networks", IEEE Communication Magazine, Vol. 40, No. 8, 2002, pp. 102–114.

[3]. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route detection and filtering of injected false data in sensor networks," in *Proc. IEEE INFOCOM*, 2004, vol. 4, pp. 2446–2457.

[4]. Wang, H. Li, Q. (2007), "PDF: A Public-key based False Data Filtering Scheme in Sensor Networks", Proceedings International Conference on Wireless Algorithms, Systems and Applications, 2007.

[5]. Karlof. Wagner, D. (2003), "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures",Proceedings of First IEEE International Workshop of Sensor Network Protocols and Applications, May 2003. pp. 113-127.

[6]. Padmavathi, G. Shanmugapriya, D. (2009), "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security(IJCSIS), Vol.4, No.1, February-2009, pp. 1-9.

[7]. Hemanta Kumar, K.Avijit Kar. (2009), "Wireless Sensor Network Security Analysis", International Journal of Next- Generation Networks (IJNGN), Vol.1, no.1, pp.1-10.

[8]. "Network Simulators", [Online] Available: http://www.isi. edu/nsnam/ns/

[9]. "Simulating Sensor Networks in NS-2", [Online] Available: http://nile.wpi.edu/NS/

[10]. Fasee Ullah. Muhammad, A. Hamid ul Ghaffar. (2010), "Simulating AODV and DSDV for A dynamic Wireless Sensor Networks", International Journal of Computer Science and Network Security, Vol.10, No.7, pp. 1-7.