Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

HMAC Filtering Scheme for Data Reporting in Wireless Sensor Network

P.Bharathi, S.Sandiya, S.Santhapreethi
Dept of IT
SM VEC, Puducherry – 605106, India

D. Balathiripurasundari
Dept. of IT
TCS Corporate, Chennai, India

Abstract— Wireless Sensor Networks consists of a large number of small sensor nodes and itself are deprived of high memory requirements, high processing power and are limited in usage of efficient security mechanisms and susceptible to possible node compromise, passive and active attacks. These restrictions make them extremely vulnerable to variety of attacks. Mostly public key cryptographic techniques are found to be more work prone with the secure exchange of keys, mainly lengthy hash operations with high processing rounds etc. Even though these technique do not provide adequate verification process of reports from source to sink nor do they completely mitigate false report injection attacks and Denial of Service attacks. In this work we propose a HMAC'ed filtering scheme for secure transmission of data and we propose a technique called Encryption of combined hashes which filters bogus reports, then specifically addresses false report injection attacks and Denial of Services. It has three phases which is Key Pre-distribution, Key Dissemination and Report Forwarding Phase. The legitimacy of the report being forwarded by the cluster head is collectively endorsed by a preset value and achieved by Message Authentication codes. In our proposed scheme increases the performance, verification is done through control messages , increases the secure data transmission and addresses the false data reports earlier.

Keywords— Wireless Sensor Network, mobile relay nodes, wireless routing, bandwidth, energy consumption.

I. INTRODUCTION

Sensor networks are dense wireless networks of small in size, very low-cost sensors, which is collect and disseminate environmental data. Wireless Sensor Networks (WSNs) facilitate monitoring and controlling of physical environments from remote locations with better accuracy. They have applications in a various fields such as environmental usage, military requirement and gathering sensing information in inhospitable places. Sensor nodes have various energy and calculating constraints because of their inexpensive nature and ad hoc method of deployment. The number of nodes in a WSN is usually much larger than that in an ad hoc network. Sensor nodes are more resource oblige in terms of power, computational capabilities, and memory. Sensor nodes are typically randomly and densely deployed (e.g., by aerial scattering) within the target sensing area. The post-deployment topology is not predetermined. Although in many cases the nodes are static in nature, the shape and size might change frequently because the sensor nodes and the wireless channels are prone to failure.

II. SYSTEM MODEL

An Some of the existing schemes for Filtering False Reports are Statistical en-route Filtering (SEF), Interleaved hop-by-hop authentication (IHA) and Providing Location aware End- to-End Data Security(LEDS). The details of these techniques are discussed briefly in the following sub-sections.

2.1 Statistical en-route Filtering (SEF)

Ye *et al.* proposed a statistical en-route filtering (SEF) scheme based on probabilistic key distribution. In SEF, a global key pool is divided into *n* partitions, each containing *m* keys. Every node randomly picks *k* keys from one partition. When some event occurs, each sensing node (that detects this event) creates a Message Authentication Code (MAC) for its report using one of its random keys. The cluster-head aggregates the reports from the sensing nodes and guarantees each aggregated report contains *T* MACs that are generated using the keys from T different partitions, where T is a predefined security parameter. Given that no more than T-1 nodes can be compromised, each forwarding node can detect a false report with a probability proportional to 1/n. The filtering capacity of SEF is independent of the network topology, but constrained by the value of n. To increase the filtering capacity, we can reduce the value of n, however, this allows the adversaries to break all partitions more easily. In addition, since the keys are shared by multiple nodes, the compromised nodes can impersonate other nodes and report some forged events that "occur" in other clusters.

2.2 Interleaved hop-by-hop authentication (IHA)

Zhu et al. proposed an interleaved hop by hop authentication (IHA) scheme. In this scheme, the base station periodically initiates an association process enabling each node to establish pair wise keys with other nodes that are t+1 hops away, where t is called as security threshold value. In IHA, each sensing node creates a MAC using one of its multihop pairwise keys, and a legitimate report should contain t+1 distinct MACs. Since every multihop pairwise key is distinguishable, IHA can tolerate up to t level compromised nodes in each cluster instead of in the whole network as SEF does. However, IHA has requires the elaborate to a fixed path for transmitting control messages between the base station and each cluster-head, which cannot be assurance by some routing protocols such as GPSR and GEAR. Moreover, the high communication overhead incurred by the association process makes IHA unsuitable for the networks whose topologies change frequently.

2.3 Providing Location aware End- to-End Data Security

Providing Location aware End-to-End Data Security (LEDS) design overcomes the limitations of the existing hop-by-hop security paradigm and achieves an efficient and effective end-to-end security paradigm in WSN. It exploits the static and location-aware nature of WSNs, and proposes a novel location-aware security approach through two seamlessly integrated building blocks: a location-aware key management framework and an end-to-end data security mechanism. In this method, each sensor node is implemented with several types of balanced secret keys, some of which intent to provide end-to-end data confidentiality, and others purpose to provide both end-to-end data authenticity and hop-by-hop authentication. All the keys are measure at each sensor node independently from keying materials pre-loaded before network deployment and the location information obtained after network disposal, without inducing new communication overhanging for shared key establishment.

III. PROBLEM DEFINITION

In this paper we discussed the existing schemes for False report Filtration. They are Statistical en-route Filtering (SEF), interleaved hop-by-hop authentication (IHA) and Providing Location aware End- to-End Data Security. Each of them address false report injection attacks and or DoS attacks. However they all have some constraints. SEF is independent of network shape and size, but it has limited number of filtering capacity and cannot prevent impersonating attacks on legitimate nodes. IHA has a drawback, that is, it must periodically establish multihop pair wise keys between nodes. Further, it refers to a located path between the base station and each cluster-head to transmit messages in both directions, which cannot be assured due to the dynamic topology of sensor networks or due to the use of some underlying routing protocol.

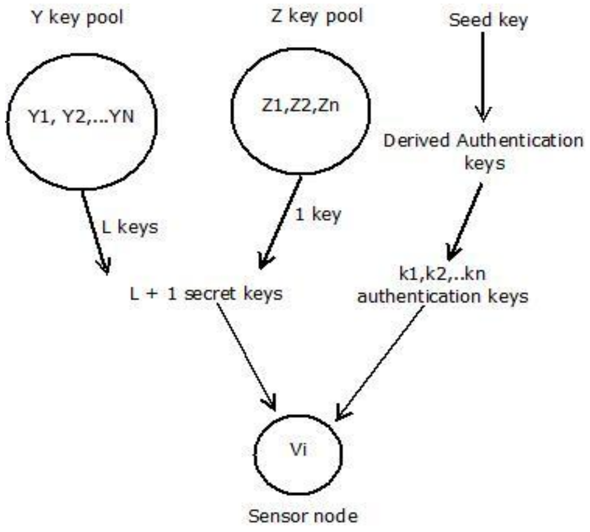
LEDS utilize location-based keys to filter false report. It assumes that sensor nodes can determine their locations in a short period of time. However, this is not practical approach, because many localization approaches take quite long and are also vulnerable to malicious attacks .It also tries to address selective forwarding attacks by allowing a whole cell of nodes to forward one report; however, this incurs high communication overhead.

IV. DESIGN

4.1 Introduction

In this chapter we describe our proposed security scheme called HMAC'ed Filtering Scheme for Data Dissemination in WSN. This scheme addresses false report injection attacks and DoS attacks such as Selective forwarding and Report disruption in WSN. The multifunctional key management framework is used in this scheme which involves authentication keys.

Similar to SEF and IHF discussed in chapter 3 our proposed en-route filtering scheme also uses the key distribution mechanism employed in WSN. Unlike other schemes which either lack strong filtering capacity or cannot support highly dynamic sensor networks, our scheme uses a hash chain of authentication keys which are used to endorse reports. Meanwhile, a legitimate report should be authenticated by a certain number of nodes. First each node disseminates its key to forwarding nodes. Then, after sending reports, the sending nodes disclose their keys, allowing the forwarding nodes to verify their reports. It can be explained with the help of the following figure 4.1.



4.2 Key Derivation

Under this scheme control messages are used to disseminate and disclose the keys to forwarding sensor nodes and later allow nodes 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 report's collective endorsement.

4.3 Problem Formulation

The vast targeted terrain where the sensor nodes are deployed is divided into multiple cells after network deployment. We assume that sensor nodes within a cell form a cluster which contains *n* nodes. In each cluster of a cell a node is randomly selected as a cluster head as in figure 4.2. When an event of interest happens in any of these cells, the sensing nodes of that particular cell detects the event and broadcast it to the cluster head. The cluster head aggregates the reports and forwards the aggregated report through the report authentication area down to the sink. The topologies of WSNs change frequently either because nodes are prone to failure or because they need to switch their states between Active and Sleeping for saving energy. As sensor networks are not tamper-resistant, it can be compromised by adversaries. Each cluster may contain some compromised nodes, which may in turn collaborate with each other to generate false reports by sharing the secret key information. In this project work we intend to provide solutions for attacks like bogus data injection and denial of services (selective forwarding attack & report disruption) that can be launched by adversaries to degrade node's life time and the critical information carried by them.

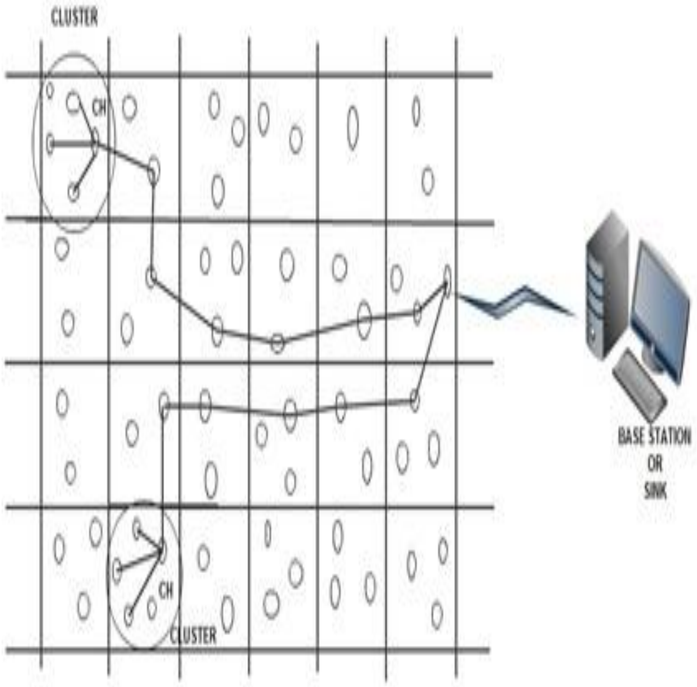


Figure 4.2: Cluster Formation and report forwarding route to Sink

We consider

N- Total no. of nodes present in the targeted terrain
n- Average no. of nodes in each cell
l- Size of the cell
t- no. of correct endorsements to validate a report
x- no. of compromised nodes in a cell

Cluster head intimates events to sink periodically & finds a routing path called Report Forward Route. We consider x nodes inject malicious data to reports periodically to drain out battery life. These x nodes inject bogus data by simply offering a wrong MAC to the collective endorsement. Due to the wrong MAC in *t* endorsements the legitimate event report has the possibility of being dropped by a legitimate node or even a legitimate report share can be dropped by an adversary near to the sink which is called Report Disruption attack. When multiple clusters disseminate keys at same time, some forwarding nodes need to store the authentication keys of different clusters. Hence the nodes closer to the base station need to store more authentication keys than others do because they are usually the hot spots and have to serve more clusters. Our aim is thus to mitigate the false data injection at early route with minimal overhead, improved network life time, confidentiality and authentication.

4.4 Design of the Project

There are 3 phases involved in the project and the relationships between them are shown in figure 4.3.

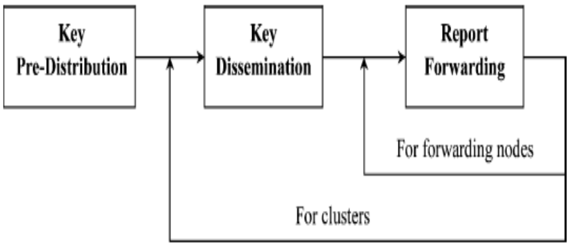


Figure 4.3: Relationship between phases

When an event occurs within some cluster, the cluster-head collects the sensing reports from sensing nodes and aggregates them into the aggregated reports. Then, it forwards the aggregated reports to the base station through a set of forwarding nodes. In our scheme, each sensing report contains one MAC that is produced by a sensing node using its authentication key (called auth-key for short), while each aggregated report contains distinct MACs depending upon the number of the cluster members.

In our scheme, each node possesses a sequence of auth-keys that form a hash chain. Before sending the reports, the cluster-head disseminates the first auth-keys of all nodes to the forwarding nodes that are located on multiple paths from the cluster-head to the base station. The reports are organized into rounds, each containing a fixed number of reports. In every round, each sensing node chooses a new auth-key to authenticate its reports.

To facilitate verification of the forwarding nodes, the sensing nodes disclose their auth-keys at the end of each round. Meanwhile, to prevent the forwarding nodes from abusing the disclosed keys, a forwarding node can receive the disclosed auth-keys, only after its upstream node overhears that it has already broadcast the reports. Receiving the disclosed keys, each forwarding node verifies the reports, and informs its next-hop node to forward or drop the reports based on the verification result. If the reports are valid, it discloses the keys to its next-hop node after overhearing.

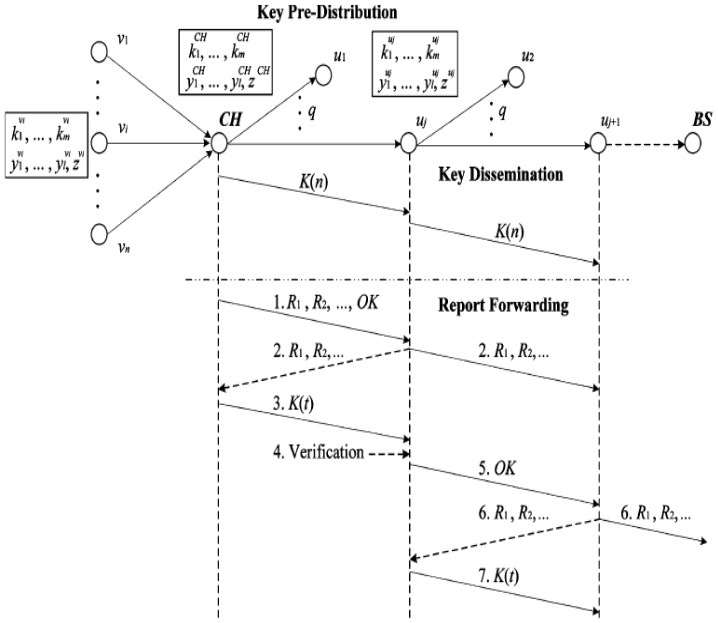


Figure 4.4: Overall process of key distribution and Report Forwarding

The processes of verification, overhearing, and key disclosure are repeated by the forwarding nodes as shown in figure 4.4 at every hop until the reports are dropped or delivered to the base station. Specifically, our scheme can be divided into three phases: (i) key pre-distribution phase, (ii) key dissemination phase, and (iii) report forwarding phase. In the key pre-distribution phase, each node is preloaded with a distinct seed key from which it can generate a hash chain of its auth-keys. In the key dissemination phase, the cluster-head disseminates each node's first auth-key to the forwarding nodes, which will be able to filter false reports later. In the report forwarding phase, each forwarding node verifies the reports using the disclosed auth-keys and disseminated ones. If the reports are valid, the forwarding node discloses the auth-keys to its next-hop node after overhearing that node's broadcast. Otherwise, it informs the next-hop node to drop the invalid reports. This process is repeated by every forwarding node until the reports are dropped or delivered to the base station.

4.5 Algorithm

STEP 1: Cluster Head (CH) collects sensing reports as in figure, from sensor nodes & generates number of aggregated reports.

R1,R2, R3,……..

CH sends these aggregated reports plus an OK message to next hop u_j.

Aggregated report must contain t Message Authentication Codes (MACs) from each sensing node with a distinct Z key. Aggregated report R looks as

$R = \{\, r(v_{i_1}), \ldots, r(v_{i_t}) \,\}$.

Where $v_{i_1}, \ldots, v_{i_t}$ denote t sensing nodes.

Since every sensing node report the same event information E, only one copy of E is kept in the aggregated report R.

STEP 2: Receiving the aggregated reports and OK , u_j forwards them to next hop, u_j+1. CH overhears the broad cast of aggregated reports from u_j.

STEP 3: Overhearing the broadcast from u_j, the CH discloses the authentication keys to u_j by message K(t)

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

Where K(t) contains authentication keys of $v_{i_1}, \ldots, v_{i_t}$. It has the same format as K (n) , but only t authentication keys.

Where K(n) is the authentication messages collected by CH from the sensing nodes and aggregated to K(n).

STEP 4: Receiving K (t), u_j first checks the authenticity of disclosed keys using the disseminated ones that it decrypted from K (n) before. Then, it verifies the integrity and validity of the reports by checking the MACs of the reports using the disclosed keys.

VERIFICATION PROCESS:

1) To verify the validity of K (t), u_j checks if K (t) is in correct format and contains t distinct indexes of z-keys (secret keys picked randomly from global key pool Z). If not, it drops K (t).
2) To verify the authenticity of the authentication keys in K (t), u_j checks if each authentication key it stored can be generated by hashing a corresponding key in K (t) in a certain number of times. If not, it is either replayed or forged and K (t) should be dropped.
3) To verify the integrity and validity of reports R1, R2… u_j checks the MACs in these reports using the disclosed authentication key that it decrypts from K (t).

STEP 5: If the reports are valid, u_j sends an OK message to u_j+1.Otherwise it informs u_j+1 to drop invalid reports.

STEP 6: Similar to step 2, u_j+1 forwards the reports to next hop.

STEP 7: Similar to step 3, after overhearing the broadcast from u_j+1, u_j discloses K (t) to u_j+1.

STEP 8: Every forwarding node repeats step 4 to step 7 until the reports are dropped or delivered to the base station.

V. SIMULATION RESULT

5.1 INTRODUCTION

In this chapter, we will start with an introduction to the simulation tool called NS-2, the ways of configuring it to run sensor networks, implementation details of the Enroute filtering scheme

5.2 SIMULATION TOOL

NS-2 is an event driven network simulator developed at University of California at Berkeley, USA, as a REAL network simulator projects in 1989 and was developed at with cooperation of several organizations. NS is not a finished tool that can manage all kinds of network model. It is actually still an on-going effort of research and development.

NS is a discrete event network simulator where the timing of events is maintained by a scheduler and able to simulate various types of network such as LAN and WPAN according to the programming scripts written by the user. Besides that, it also implements variety of applications, protocols such as TCP and UDP, network elements such as signal strength, traffic models such as FTP and CBR, router queue management mechanisms such as Drop Tail and many more.

There are two languages used in NS-2; C++ and OTcl (an object oriented extension of Tcl). The compiled C++ programming hierarchy makes the simulation efficient and execution times faster. The OTcl script which written by the users the network models with their own specific topology, protocols and all requirements need. The form of output produce by the simulator also can be set using OTcl. The OTcl script is written which creating an event scheduler objects and network component object with network setup helping modules. The simulation results produce after running the scripts can be use either for simulation analysis or as an input to graphical software called Network Animation (NAM).

1 .configuration of sensor network simulations:

Setting up a sensor network in ns-2 follows the same format as mobile node simulations. Places where a sensor network simulation differs from a mobile node simulation are listed below.

1. Configuration of Phenomenon channel and Data channel.
2. Configuration of Phenomenon nodes with the PHENOM "routing" protocol.
3. Configuration of Phenomenon node's pulse rate and phenomenon type.
4. Configuration of Sensor nodes.
5. Attaching sensor agents.
6. Attaching UDP agent and sensor application to each node.
7. Starting the Phenomenon node.
8. Starting the Sensor Application.

2. Implementation Details Of Hmac'ed Filtering Scheme

2.1 Implementation Of Md5 Hashing Technique

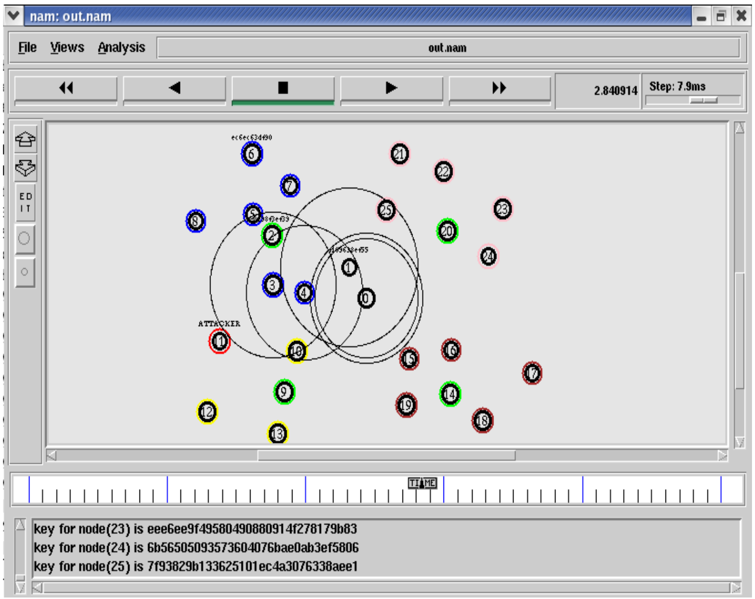
MD5 Hashing technique is used to produce hash of the sensor report. To accomplish this task MD5 algorithm is implemented in tcl script for Ns-2 simulation. The steps describing its process are listed below

1. Append the padding bits
2. Append length
3. Initialize the Message Digest buffer
4. Process the message in 512 bit blocks
5. Resultant 128 bit Message Digest.

3. Implementation of Key Comparison Process And Report Delivery

As the reports are sent in rounds containing distinct *n* number of reports, it is not needed to send the whole *K (t)* which contains all the first authentication keys of the sensor nodes. Instead we can send alone the *n* number of *t* authentication keys which will now enhance faster deciphering of the MAC-ed reports. In order to filter the false packets at the earlier route, this K (n) is discarded in the nodes nearer to the sink. The above said process is accomplished in the following ways. Keys are randomly picked up from a matrix and they are used for producing HMAC of the report. The cluster head now receives all the first authentication keys from the cluster members and pack them in K (n) and send to the Report forwarding nodes.

The Cluster members sense the events and produce HMAC of the report and then send them collectively to Cluster Heads. The Cluster head now collectively endorse the received HMAC's with the preset value. The comparison of keys in K(n) and the key obtained from HMAC 'ed report are verified and forwarded by the cluster heads to their one hop report forwarding nodes . When the HMAC offered by a sensor node is found to be illegitimate, i.e., if the key found in the HMAC is different from the collectively endorsed report, cluster head marks node as attacker which is shown in Figure 5.1.



```
key for node(23) is eee6ee9f49580490880914f278179b83
key for node(24) is 6b56505093573604076bae0ab3ef5806
key for node(25) is 7f93829b133625101ec4a3076338aee1
```

Figure 5.1: Identification of Attacker through collective endorsement

4 Implementation of Collective Endorsement Of Sensor Reports.

Sensor Reports are HMACed as the result of HMAC algorithm implemented in TCL script with the keys randomly picked up from the assigned key matrix. Those reports are further divided into small authenticated shares in the range of 16 bytes each and are sent in rounds from the cluster members to the cluster head in order to prevent Report disruption attack.

A Report disruption attack when launched by an attacker will make the complete legitimate share of sensor report abruptly dropped by a legitimate cluster head by simply offering an illegitimate MAC to the collective share. Hence through collective endorsement the whole sensor reports are further divided into small authenticated shares such that even when an attacker offers illegitimate HMAC the cluster head can able to recover the complete collective share with the help of legitimate shares received from its members.

5. Simulation Environment

The proposed secure scheme of Dynamic enroute filtering is implemented in ns-2.27 simulator. The simulation consists of 24 sensor nodes out of which 4 nodes in green color are cluster heads, some nodes are configured to be attackers and a base station are randomly deployed in a terrain dimension of 600m X 600m with the following simulation environment shown in Table 5.2.

Table 5.2: Simulation Environment

PARAMETER	**VALUE**	**DESCRIPTION**
Channel	*Channel/Wirelesschannel*	Channel Type
Propagation	*Propagation/TwoRayGround*	Radio Propagation Model
Network Interface	*Phy/WirelessPhy*	Network Interface Type
MAC	*Mac/802_11*	Medium Access Control Type
Interface Queue	*Queue/DropTail*	Interface Queue Type
Link Layer	*LL*	Link Layer
Antenna	*Antenna/OmniAntenna*	Antenna Model
Interface Queue Size	*5000(in packets)*	Maximum packet in interface Queue
Routing Protocol	*AODV*	Routing Protocol
Data Rate	*11Mbps*	Data Transfer Rate
Interface Queue Size	*50*	Maximum packets in Interface Queue.
Terrain Dimension	*600m X 600m*	Terrain Dimension of the network
Simulation Time	*100 Seconds*	Total duration of the simulation
Packet Size	*1026Bytes*	Size of the CBR traffic packet
Number of Nodes	*25*	Number of nodes in the Scenario
Energy Model	*Reception- rx Power 0.3(J/bits) Transmission- tx Power 0.5(J/bits)*	Power Consumption Model

6 .Performance Metrics & Evaluation

The performance metrics are ought to be used to measure the performance of the proposed system.

1 Filtering capacity

Filtering capacity of the proposed scheme is defined as the average number of hops that a false report can be detected by the forwarding node at every hop or the fraction of number of false report filtered to the number of hops travelled.

2 Energy savings

Energy savings of the proposed scheme is defined as the energy consumption in transmission, reception and the computations due to the extra fields which incurs extra overhead. We evaluate the length of a normal report without using any filtering scheme and then compare the length of an authenticated report in the next phases of the review.

Performance metrics determine the performance of a particular scheme in the presence of constrains related to domain oriented advantages and drawbacks. We have evaluated our Enroute mechanism in terms of Throughput, Packet loss.

3 Packet losses

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. It can be evaluated with the formula given below.

Packet Loss (in packets) = DataAgtSent − DataAgt Rec

Where AGT– agent trace (used in new trace file format)

Scenario: Packet Loss Vs Number of Attacker nodes:

Same scenario is maintained in which Packet loss is computed by varying the number of attackers. As shown in Figure 5.3, packet loss seems to be very high when there is increase in the attacker's 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 as discussed in the Threat and Trust model of chapter 2. With Enroute Filtering mechanism packet loss is reduced to 40% which is achieved by the identification of attacker nodes through collective endorsement implemented in the cluster heads.

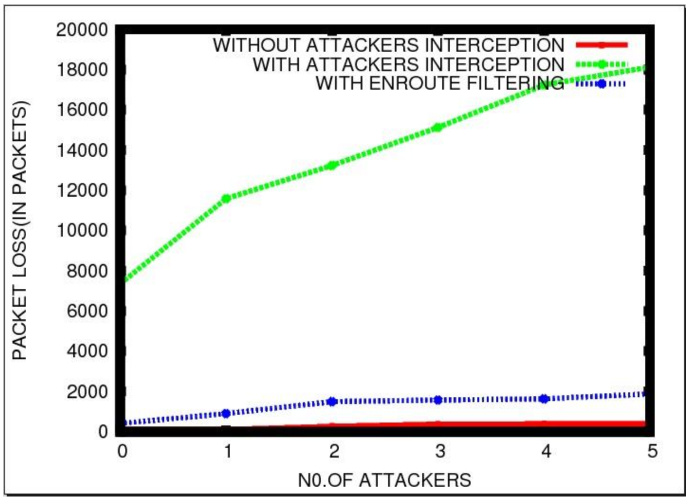


Figure 5.3 Packet Loss Vs Number of Attacker node

VI. CONCLUSION

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 adversary's activities. Hence this enroute filtering scheme is currently an area of much research among the security professionals. Even though there are routing protocols available for the sensor networks, AODV performs better than many other on-demand protocols under high mobility, large network scenarios. When the size of the network is large and highly mobile the frequency of the link failure is also high. Due to this, latency and control load of the network is also increased. Also due to the attacker's single illegitimate MAC there is a threat of dropping the complete legitimate share. Hence the future works can be emphasized more on the efficient filtering of the false report even at such conditions. Also the future works can be extended to implement such secure schemes on the security protocols available for sensor networks keeping the energy constraint as main criteria.

We in this work, proposed a HMAC'ed filtering scheme for WSN that utilizes the dissemination of authentication keys for filtering false data injection attacks and DoS attacks. In our scheme, each node uses its own authentication keys to authenticate their reports and a legitimate report should be endorsed by *t* nodes. The authentication keys of each node form a hash chain and are updated in each round. The Enroute scheme also yielded a better attacker detection and mitigation framework together with disseminated key structure. We thus analyzed the performance metrics of the Enroute Filtering scheme with AODV protocol in terms of Throughput and Packet Loss and their results are also discussed. In future we intend to compare the performance of Enroute Filtering Scheme implemented with the security protocols such as SPINS etc.

REFFERENCE

[1] Yun Zhou, Yuguang Fang, and Yanchao Zhang, "Securing wireless sensor networks: a survey", IEEE Communications Surveys & Tutorials, Vol.10, No. 3, pp.6-28, September2008.

[2] Al-Sakib Khan, Pathan,Hyung-Woo Lee, and Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International Conference on Advanced Computing Technologies, Vol. 4, No.1, pp. 1043-1045, April 2006.

[3] Zoron S.Bojkovic, Bojan M.Bakmaz, Miodrag, and R.Bakmaz, "Security Issues in Wireless Sensor Networks", International journal of Communications, Vol. 2, no.1, pp.106-114, June 2008.

[4] Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," In Proceedings of First IEEE International Workshop of Sensor Network Protocols and Applications, Vol. 1, pp.113-127 May 2003.

[5] H. Fang, F. Ye, Y. Yuan, s. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks", In proceeding of ACM international symposium on Mobile ad hoc networking and computing, Vol. 3, pp. 14-27, June 2003.

[6] F.L. Lewis "Wireless Sensor networks" Available: http://arri.uta.edu/acs

[7] G. Padmavathi and Mrs. D. Shanmugapriya, "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, pp. 1-9, February-2009.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communication Magazine, Vol. 40, No. 8, pp. 102–114, August, 2002.

[9] Hemanta Kumar Kalita, and Avijit Kar, "Wireless Sensor Network Security Analysis" International journal of Next-Generation Networks(IJNGN), Vol.1, no.1, pp.1-10, December 2009.

[10] Elaine shi and Adrian perrig, "Designing secure sensor networks", IEEE wireless communications, Vol. 2 pp. 38-43, December 2004.

[11] Haowen Chan, Adrian Perrig, and Dawn Song, "Random Key Pre distribution Schemes for Sensor Networks", In Proceedings of IEEE Symposium on Security and Privacy, Vol. 3, pp.1-17, September 2003.

[12] F. Ye, H. Luo, S. Lu, and L. Zhang "Statistical en-route detection and filtering of injected false data in sensor networks," In Proceedings of IEEE INFOCOM, Vol.4, pp. 2446–2457, September 2004.

[13] 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 Proceedings of IEEE Symposium on Security and Privacy, Vol.4, pp. 259–271, August 2004.

[14] Kui Ren, Wenjing Lou, and Yanchao Zhang, "LEDS: Providing Location-aware End-to-end Data Security in Wireless Sensor Networks", In Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM) pp. 1-12, April 2006.

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

[16] Nor Surayati Mohamad Usop, Azizol Abdullah, and Ahmad Faisal Amri Abidin "Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment" IJCSNS International Journal of Computer Science and Network Security, Vol.9 No.7, pp 261-268 July 2009.

[17] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar "SPINS: Security Protocols for Sensor Networks", In Proceedings of Mobicom 2001, Vol 8, No.5, pp. 521-534, September 2002.

[18] Gowrishankar.S, SubirKumarSarkar T.G.Basavaraju "Scenario Based Simulation Study of Adhoc Routing Protocol's Behavior in Wireless Sensor Networks", 2009 International Conference on Future Computer and Communication, Vol.5, No.4, pp 527-532, July 2009