Secured Data Dissemination in Wireless Sensor Networks

[1]Parthiban.N, [2]J.Godwin Ponsom

[1]Student, [2]Assistant Professor
[1]Department of Information Security and Cyber Forensics, SRM University, Kattankulathur, Chennai, T.N., INDIA
[2]Department of Information and Technology, SRM University, Kattankulathur, Chennai, T.N., INDIA
[1]thiban_45@yahoo.co.in, [2]godwinsrm@gmail.com

***Abstract*— Wireless Sensor Networks are less used because of lack of good security mechanism, need to high power and memory requirement and is too vulnerable to many kinds of attacks, so most of the security mechanism focus on cryptographic techniques, key exchange, and hashing techniques. And off Couse there came many security mechanism and surveys that provided techniques and mechanisms to mitigate attacks against false injection attack and dos attacks, etc., moreover even these proposed security mechanisms only concentrated on the mitigating process for the complete data travel, i.e. the en-route and thereby left to be still at high risk , So in this paper , we came up with a contrivance that does secured dissemination thought out the en-route , thereby reducing the false filtering mechanism with the help of Nested HMAC structures. This is done by the keys derived by the nodes and cluster members. As a whole we reduce potential attacks and dos attack, and do compare with the existing methodologies which tried to reduce the same, tag an attacker as malicious node once if it is found to be the attacker, thereby alerting the sink . The correctness of the data being forwarded by the cluster head is collectively endorsed by Message authentication codes. We evaluate and analyze the performance of our mechanism through extensive analysis of relocating the position of malicious nodes in the event area.**

***Index Terms*— WSNs, Security, False injection and DOS attacks.**

I. INTRODUCTION

. A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on, A WSN node contains several technical components. These include the radio, battery, microcontroller, analog circuit, and sensor interface. When using WSN radio technology, you must make important trade-offs. In battery-powered systems, higher radio data rates and more frequent radio use consume more power, their exist a lot of methodology trying to solve the problems related to the filtering of the fake reports such as IHA,LEDS , LBRS, SEF and CCEF etc. but all proposed mechanism have certain disadvantages incorporated in it, Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited for the unique features and application requirements of sensor networks. The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network. Hence the following features are the highly vulnerable areas where attacks can be possible at adverse conditions.

In the rest of this project we discuss in a systematized manner as follows. In Section II, we discuss the work regarding the secured data broadcasting. The safety and threat prototypes are discussed in Section III. In Section IV, we represent the particulars of our planned work with algorithms and problem formulation. In section V, we estimate the efficiency of our projected algorithms using network simulations and at last in Section VI, we conclude with the discussions on future work of our project.

II. RELATED WORKS

Some currently existing methodologies to mitigate these specified attacks are Static Enroute filtering mechanism (SEF), Location aware end to end data security(LEDS), Interleaved hop by hop authentication(IHA), etc., so following briefs out the working and its disadvantages, in SEF a key pool is grouped into n groups, each accumulating m keys, thereby selecting a key from each group, when it senses some event or occurrences it creates a MAC for the sensed data using the acquired key, then the cluster head aggregates the data and validates its legitimacy ,by guarantying that there is T MACs generated by each key from distinct groups, to increase the filtering capacity , we can decrease n, but still it's easy to impersonate other nodes. IHA has a drawback, that is, it must periodically establish multihop pair wise keys between nodes. Moreover, it asks for a fixed path between the base station and each cluster-head to transmit messages in both directions, which cannot be guaranteed 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, 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.

III. SECURITY AND THREAT MODEL

We deploy nodes in the area where we are interested, like detecting of CO, etc., when the nodes senses the presence of co, all the nodes which detected will send the message to the cluster head, this CH act as a master for the some group of cluster, they are elected using difference criteria or parameters like energy etc., this sensed message is then sent to base station via the en-route nodes, here our potentially concentrate on False injection attack and dos attack.

False report injection attacks

It's an attack in which an adversary injects fabricated reports into the network with the goal of deceiving the base station or of draining the energy resources.

DOS attacks

Under this, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any more selective forwarding attack and 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.

IV. PROPOSED SYSTEM

In this paper, we make use of nested MAC to add attacker detecting, strength to add confidentiality and bogus data filtering capacity thereby ensuring end to end data security of the data delivered to the sink, MAC structure is used to handle the authentication keys of the nodes, the number of authentication keys validating process is reduced to the number equivalent to number of CH for making the filtering of false data faster. In this scheme control messages are used to disseminate and disclose the keys to forwarding nodes and allowed later finding a shared secret key and verify the keys by decrypting them. To do this we maintain two secret key pools and a seed key, and from that a series of authentication keys are derived as needed, thereby wen a shared secret key its corresponding authentication keys are derived and kept in memory of the nodes. Later those keys are used for encrypting the authentication keys which are used for producing the MAC

Assumptions:

Before the sensor nodes are being deployed in the terrain, all the nodes are pre-loaded with the 2 secret key pools and seed key, the communication for each node is limited only to certain distance of radius r, i.e. the transmission range. Thus the communication is carried out only if the nodes are within its range. Out of the nodes from the cluster one node is opted as a cluster head depending on many reason like power, memory etc., the CH does the same work as a member of a cluster and has no difference. Let's assume out topology to be very dynamic and is subjected to change in the position because of the nature of the sensor nodes and it can change between active and sleep mode when it is inactive.

Phases of Secured Data Dissemination:

The whole securely disseminating of data from the CH to the sink is carried out in four major phases. They are 1.key pre distribution phase, 2. Cluster head verification, 3.key dissemination, 4.verification and report forwarding phase, in the first phase all the mandatory keys needed for the communication is preloaded in the deployment. The second phase deals with the validation of the nested HMAC of the report. The third phase segregates the authentication keys derived and are disseminated to the forwarding nodes

Key Pre-Distribution:

In this phase seed keys are loaded in the nodes before deploying in the terrain, using a common hashing technique such as MD5 sequence of pre-authentication keys can be formed. Let 'm' be the length of the hash chain formed. Let Vi be the node 4, and its corresponding seed key is k_m^{vi} , from which we can derive the pre-authentication keys can be deduced as follows:

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

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

.....

.....

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

Whereas Vi is the node's index and $h^2(k_m^{vi})$ denotes hashing k_m^{vi} . Apart from the seed key each node is loaded with two key pools Y and Z, shown in figure below. From Y we take 'l' keys and a single key from Z key pool. Along n nodes of a cluster, it is assumed that there are at least t nodes having a distinct z-key. Hence a cluster member's pre-authentication keys are, $k_{1,\ldots\ldots}^{vi} k_m^{vi}$. .and the secret keys are $y_1^{vi}, \ldots\ldots y_l^{vi}$ and z^{vi}

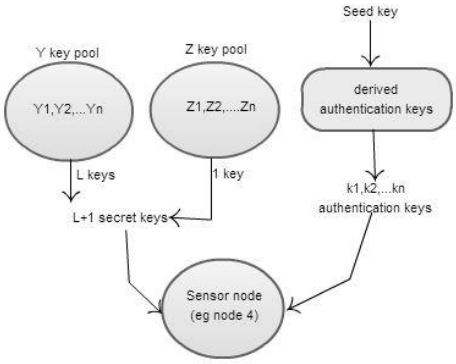

Figure: 1 Node with key pools

Cluster Head Verification:

Nested HMAC is produced using the pre-authentication keys derived from the seed key which is later encrypted using l+1 secret keys. Its Representations are specified below as follows.
iv = node 4.
H= hash function MD5.
M= data to HMAC.
N_{EHF}= length of hash code produced hash function (MD5).
k_{auth}= authentication key as a result of encryption of pre authentication key and secret keys.
$k^+ = k_{auth}$ padded with zeros so that the result is equal to number of bits in the message block.
Finally the Nested HMAC'ed report can be expressed as below.

$$HMAC\ k_{auth} = H[(K + \oplus\ opad) + H[(K + \oplus\ ipad) + M]] \text{ ----------->> (1)}$$

The sensed data and the nested HMAC are sent to the CH by the members of the cluster. Before sending the data acquired by cluster head, it sends 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.

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

$$K(n)=\{k_{auth_{v1}}, \ldots . k_{auth_{vn}}\} \text{ ----------->>>(2)}$$

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 $K(n)=\{k_{auth_{v_{i2}}}, \ldots . k_{auth_{v_{it}}}\}$ ---------->> (3)

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. It 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.

Proposed Algorithm:

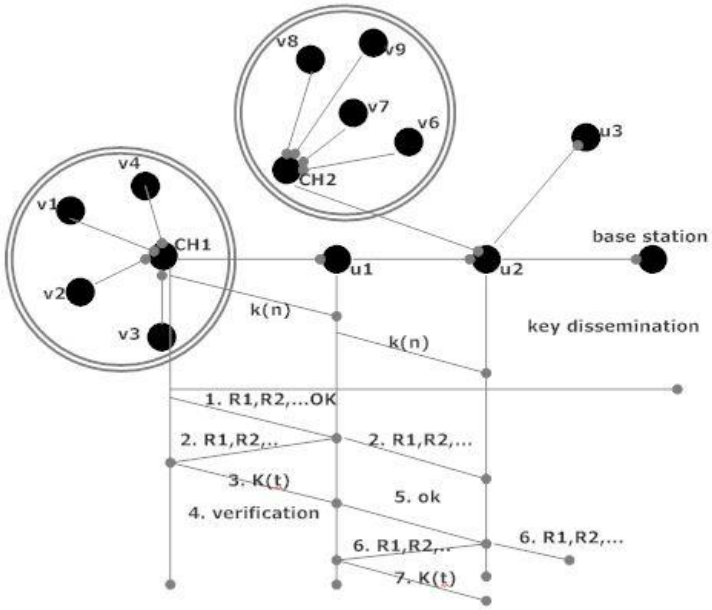

Figure 2: key distribution and report forwarding

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.

Algorithm 1: Cluster Head

1: For $i = 1$ to l do
2: Collect $r[i] + M$ from $n[i]$
3: //this Produce Nested $HMAC\ [M]$
4: $HMAC\ k_{auth} = H[(K + \oplus\ opad) + H[(K + \oplus\ ipad) + M]]$
5: Compare computed HMAC with Produced HMAC.
6: If $HMAC\ k_{auth}$ is valid
7: //Aggregate the report.
8: Report $R = r(v_{i1}), \ldots, r(v_{in})$
9: Discard redundant $r[i]$
10: End if.
11: End for.
12: //Collect Authentication keys k_{auth} from n[i].
13: K(n)=$\{k_{auth_{v1}}, \ldots . k_{auth_{vn}}\}$
14: Select Report Forward Nodes to q.
15: Disseminate $K(n)$ to q
16: Forward R to .
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 HMA
10: If $HMACk_{auth}$ 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

V. SIMULATION RESULT

We have used NS-2 for the simulation of the proposed scheme. Sensor network packages are configured 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 Table 1. The simulation consists of 25 sensor nodes out of which 4 nodes are set to be cluster heads i.e., four clusters are grouped with a cluster head and cluster members. Out of those 24 nodes some nodes are configured to be malicious and their intention was set to drop the packets there by launching false data injection attack and Dos attacks..

Table 1: Simulation Parameters

Simulation Area	1000 m x 1000 m
Number of sensor nodes	25
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	1000 bytes
Simulation Time	100 seconds

. The routing protocol adopted in our simulation is AODV (Ad hoc On demand Distance Vector). We preferred AODV as routing protocol because it does not need any central administrative system to control the routing process. The packet delivery efficiency is more than other proposed models. The proposed system prevents false injection attacks, report disruption attack; DOS attacks like selective forwarding are prevented to a great extent. Since nested HMAC is being used, the transportation of keys among the nodes is fully secured. This renders the key useless for the attacker. The simulation also shows that the proposed system increases the throughput and a high reduction in control messages is observed. Average End-to-End Delay is also reduced on implementing the above proposed system

VI. CONCLUSIONS AND FUTURE ENHANCEMENTS

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. 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 attackers 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. We in this work proposed a secured data dissemination with en-route 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 Average End to End Delay and Packet Delivery Ratio, 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

REFERENCES

[1] 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.
[2] Zhou, Y. Fang, Y. Zhang, Y. (2008), "Securing Wireless Sensor Networks: a Survey", IEEE Communications Surveys & Tutorials, Vol.10, No. 3, 2008, pp.6-28.
[3] Al-Sakib Khan, Pathan, Hyung-Woo Lee, Seon Hong, C. (2006),"Security in Wireless Sensor Networks: Issues and Challenges", Proceedings International Conference on Advanced Computing Technologies, April 2006, pp. 1043-1045.
[4] Zoron Bojkovic, S. Bojan Bakmaz, M. Miodrag, Bakmaz, R. (2008),"Security Issues in Wireless Sensor Networks",International Journal of Communications, Vol.2, No.1, 2008, pp.106-114.
[5] Ye, F. Luo, H. Lu, S. Zhang, L. (2004), "Statistical E-route Detection and Filtering of Injected False Data in Sensor Networks", Proceedings IEEE International Conference on Computer Communications (INFOCOM 2004), Vol.4, September 2004, pp. 2446–2457.
[6] Zhu, S. Setia, S. Jajodia, S. Ning, P. (2004), "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks", Proceedings IEEE Symposium on Security and Privacy, Vol.4, August 2004, pp. 259–271.
[7] Karp, B. Kung, H.T. (2000),"GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", Proceedings ACM MobiCom, 2000, pp. 243–254.
[8] Yang, H. Lu, S. (2004), "Commutative Cipher based Enroute Filtering in Wireless Sensor Networks", Proceedings IEEE VTC 2004, Vol. 2, March 2004, pp. 1223–1227.
[9] Kui Ren, Lou, W. Zhang, Y. (2006), "LEDS: Providing Location-aware End-to-End Data Security in Wireless Sensor Networks", Proceedings 25th IEEE International Conference on Computer Communications (INFOCOM 2006), April 2006, pp. 1-12.
[10] Eschenauer, L. Gligor, V.D. (2002), "A Key Management Scheme for Distributed Sensor Networks", Proceedings 9th ACM Conference on Computer and Communication Security, November 2002.
[11] Stajano, A. Anderson, R. (1999),"The Resurrecting Duckling: Security Issues for Ad Hoc Networks". Proceedings International Workshop on Security Protocols, July 1999.