Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Object Oriented Approach to Dynamic En-Route Filtering Scheme for Data Reporting in Wireless Sensor Networks

T Anusha
Asst. Professor,
Dept. of School of Computing,
Gokaraju Rangaraju Institute of Engineering and Technology,
Hyderabad, India

K Butchi Raju
Assoc. Professor,
Dept. of School of Computing,
Gokaraju Rangaraju Institute of Engineering and Technology,
Hyderabad, India

Sk Althaf Hussain Basha
Professor, Dept. of School of Computing,
Gokaraju Rangaraju Institute of Engineering and Technology,
Hyderabad, India

Vijay Kumar Gongale
Software Engineering
NET ENRICH, Hyderabad, India

Abstract—Wireless Sensor Network (WSN) is always a challenging concept in computer networks due to the constraints such as memory, power and processing capabilities. One of the main key issues in this is Filtering Scheme for Data reporting. Presently, 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. In this paper deals with a dynamic en-route filtering scheme that addresses both false report injection and DoS attacks in wireless sensor networks. This scheme, each node has a hash chain of authentication keys used to endorse reports; meanwhile, a legitimate report should be authenticated by a certain number of nodes. Our Experimental results show that compared to existing solutions, our scheme can drop false reports earlier with a lower memory requirement, especially in highly dynamic sensor networks.

Key words— Wireless Sensor Network (WSN), DOS; Filtering; Dynamic enroute; Object oriented.

I. INTRODUCTION

Recently convergence of technological and application trends has resulted in an exceptional level of interest in wireless ad hoc networks and in particular in wireless sensor networks (WSNs). The push was provided by rapid progress in computations and communications technology as well as the emerging field of lower cost, reliable, MEMS-based sensors. The pull was provided by numerous applications that can be summarized under the umbrella of computational worlds, where the physical world can be observed and influenced through the Internet and WSN infrastructures. Consequently, there have been a number of vigorous research and development efforts at all levels of development and usage of WSNs, including applications, operating systems, architectures, middleware, integrated circuits, and systems. Typically, WSNs contain hundreds or thousands of sensor nodes that have the ability to communicate with each other [1]. While the sensor nodes have limited sensing region, processing power and energy, networking a large number of such nodes gives rise to a robust, reliable and accurate sensor network covering a wider region. Since the sensor nodes are energy-constrained, a typical deployment of a WSN poses many challenges and necessitates energy-awareness at all layers of the networking protocol stack. In these scenarios, sensor networks may suffer different types of malicious attacks. One type is called false report injection attacks [2], 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. Also, the adversaries may launch DoS attacks against legitimate reports. In selective forwarding attacks [3], they may selectively drop legitimate reports, while in report disruption attacks [4], they can intentionally contaminate the authentication information of legitimate reports to make them filtered out by other nodes. Therefore, it is very important to design a dynamic quarantine scheme to filter these attacks or at least mitigate their impact on wireless sensor networks. Recently, several schemes such as SEF [5], IHA [2], CCEF [6], LBRS [4], and LEDS [3] have been proposed to address false report injection attacks and/or DoS attacks. However, they all have some limitations. In this paper, deals with a dynamic en-route filtering scheme to address both false report injection attacks and DoS attacks in wireless sensor networks. In our scheme, sensor nodes are organized into clusters. Each legitimate report should be validated by multiple message authentication codes (MACs), which are produced by sensing nodes using their own authentication keys. The authentication keys of each node are created from a hash chain. Before sending reports, nodes disseminate their keys to forwarding nodes using Hill Climbing approach. Then, they send reports in rounds. In each round, every sensing node endorses its reports using a new key and then discloses the key to forwarding nodes. Using the disseminated and disclosed keys, the forwarding nodes can validate the reports. In our scheme, each node can monitor its neighbors by overhearing their broadcast, which prevents the compromised nodes from changing the reports. Report forwarding and key disclosure are repeatedly executed by each forwarding node at every hop, until the reports are dropped or delivered to the base station.

II. LITERATURE SURVEY

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. presented a Statistical En-route Filtering (SEF) scheme [5] based on probabilistic key distribution. In Statistical En-route Filtering, a global key pool is divided into partitions, each containing keys. Every node randomly picks keys from one partition. When some event occurs, each sensing node (that detects this event) creates a MAC for its report using one of its random keys. Yang et al. proposed a Commutative Cipher Based En-route Filtering (CCEF) scheme [6]. In Commutative Cipher Based En-route Filtering, each node is preloaded with a distinct authentication key. When a report is needed, the base station sends a session key to the cluster-head and a witness key to every forwarding node along the path from itself to the cluster-head.

Yang et al. further presented a Location-Based Resilient Security (LBRS) solution [4]. In Location-Based Resilient Security, a sensing field is divided into square cells, and each cell is associated with some cell keys that are determined based on the cell's location. Each node stores two types of cell keys. One type contains the keys bounded to their sensing cells to authenticate the reports from those cells. The other type contains the keys of some randomly chosen remote cells, which are very likely to forward their reports through the node's residing cell. Recently, Ren et al. presented a Location-Aware End-to-End Data Security (LEDS) scheme [3] that can address false report injection and some DoS attacks. Like LBRS, LEDS assumes that sensor nodes can generate the location-based keys bounded to cells within a secure short time slot. LEDS provides end-to-end security by allowing sensing nodes to encrypt their messages using the cell keys. Alegitimate report contains distinct shares produced from the encrypted message using nodes' secret keys. Several distributed distance-vector based routing protocols [7] have been designed and implemented in TinyOS [8]. 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.

GEAR [9] and GPSR [10] are location-aware routing algorithms, which assume that each node is aware of its own location. Route is determined as the neighbor with the shortest distance to the sink. If all neighbors are farther than a node itself, the node uses a right-hand rule to select the route. In GEAR, the energy level of each neighbor is also taken into consideration in route selection. One observation from GPSR/GEAR is that the path between two nodes is not bidirectional, i.e., the reports from node to may choose a different path from that chosen by the reports from node to .

Braginsky *et al.* presented Rumor [11] routing protocol. In this Rumor routing protocol, when a sensing node detects some event, it creates an agent that is actually a message containing the routing information about the event. The agent follows a straight path to leave from the sensing node and is associated with a maximum TTL. Each node passed by the agent learns the route to the event. If the base station is interested in some event, it sends out a query message. The movement pattern of a query message is similar to that of an agent. When a query message is delivered to a node who knows the route to the event, a path between the base station and the sensing node (the event) can be established.

Although we only discussed a few routing protocols, our scheme can take advantage of any routing protocol that is designed for wireless sensor networks instead of only the protocols we discussed.

III. PROPOSED SYSTEM ARCHITECTURE

A. Existing System:

Recently, various approaches/schemes have been proposed(eg., SEF, IHA, CCEF, LBRS , and LEDS) to address false report injection attacks and/or DoS attacks. However, they all have some limitations. SEF is independent of network topology, but it has limited filtering capacity and cannot prevent Impersonating attacks on legitimate nodes. Interleaved hop-by-Hop authentication scheme (IHA) has a drawback, that is, it must periodically establish multihop pairwise 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 such as GPSR. CCEF also relies on the fixed paths as IHA does and it is even built on top of expensive public-key operations. More severely, it does not support en-route filtering. LBRS and LEDS utilize location-based keys to filter false reports. They both assume 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. In Location-Based Resilient Security, report disruption attacks are simply discussed, but no concrete solution is proposed. Location-Aware End-to-End Data Security tries to address selective forwarding attacks by allowing a whole cell of nodes to forward one report, however, this incurs high communication overhead.

B. Proposed System/approach:

In this paper, we deals an approach , a dynamic en-route filtering scheme to address both false report injection attacks and DoS attacks in wireless sensor networks. In our scheme/approach, sensor nodes are organized into clusters. Each legitimate report should be validated by multiple message authentication codes (MACs), which are produced by sensing nodes using their own authentication keys. The authentication keys of each node are created from a hash chain.

Before sending reports, nodes disseminate their keys to forwarding nodes using Hill Climbing approach. Then, they send reports in rounds. In each round, every sensing node endorses its reports using a new key and then discloses the key to forwarding nodes. Using the disseminated and disclosed keys, the forwarding nodes can validate the reports. In our scheme, each node can monitor its neighbors by overhearing their broadcast, which prevents the compromised nodes from changing the reports. Report forwarding and key disclosure are repeatedly executed by each forwarding node at every hop, until the reports are dropped or delivered to the base station. Figure 1 shows Sensor nodes are organized into clusters. The big dashed circles outline the regions of clusters. CH and BS denote Cluster-Head and Base Station respectively. u1~ u5are forwarding nodes, and v1~v8are sensing nodes (they can also serve as forwarding nodes for other clusters). The black dots represent the compromised nodes, which are located either within the clusters or en-route.

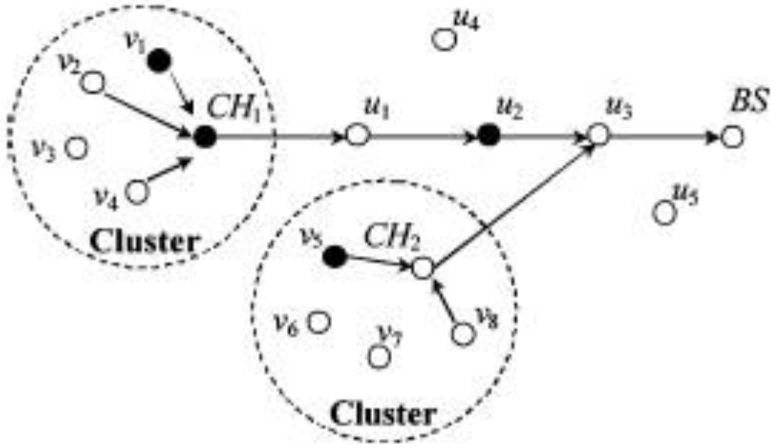


Fig 1 Sensor Cluster Structure

i. System features:

1. Neighborhood management essentially has three components: insertion, eviction, and reinforcement.
2. For each incoming packet upon which neighbor analysis is performed, the source is considered for insertion or reinforcement.
3. If the source is represented in the table, a reinforcement operation may be performed to keep it there.
4. If the source is not present and the table is full, the node must decide whether to discard information associated with the source or evict another node from the table.
5. We seek to develop a neighborhood management algorithm that will keep a sufficient number of good neighbors in the table regardless of cell density.

C. OUR SCHEME

Figure 2 the relationship between three phases of our scheme. Key pre distribution is preformed only once. Key dissemination is executed by clusters periodically. Report forwarding happens at each forwarding node in every round.

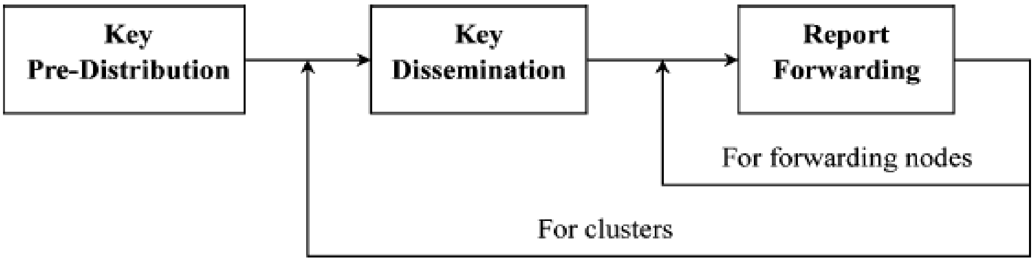


Fig 2 cluster stages in our approach

Specifically, our scheme can be divided into three stages: key pre distribution stage, key dissemination stage, and report forwarding stage. In the key pre distribution stage, 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. Fig. 2 demonstrates the relationship between the three phases of our scheme. Key pre distribution is performed before the nodes are deployed, e.g., it can be done offline. Key dissemination happens before the sensing nodes begin to send the reports. It may be executed periodically depending on how often the topology is changed. Every time the latest (unused) auth-key of sensing nodes will be disseminated. Report forwarding occurs at each forwarding node in every round.

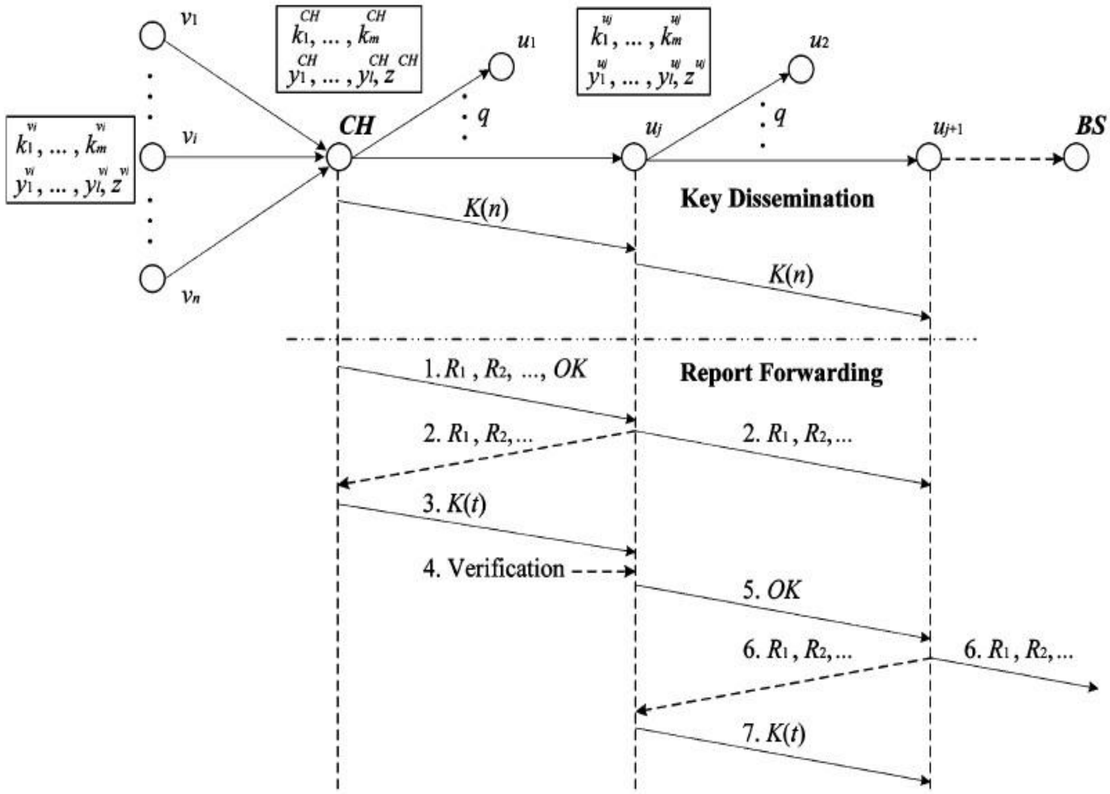


Fig 3 Detailed Procedure for our scheme

D. KEY PRE DISTRIBUTION SCHEME

Fig. 3 shows the detailed procedure of three phases.

In the key pre distribution stage, each node is preloaded with l+1 secret keys y_1,………… ,y_l and z, and can generate a hash chain of auth-keys $k_1 \dots k_m$ from the seed key k_m .

In the key dissemination stage, the cluster-head disseminates the auth-keys of all nodes by message K(n) to q downstream neighbor nodes. Every downstream node decrypts some auth-keys from K(n), and further forwards K(n) to q more downstream neighbor nodes, which then repeat the same operation.

In the report forwarding stage, each forwarding node en-route performs the following steps:

- It receives the reports from its upstream node.
- If it receives confirmation message OK then forwards the reports to its next-hop node. Otherwise, it discards the reports.
- It receives the disclosed auth-keys within message K(t) and verifies the reports by using the disclosed keys.
- It informs its next-hop node the verification result.

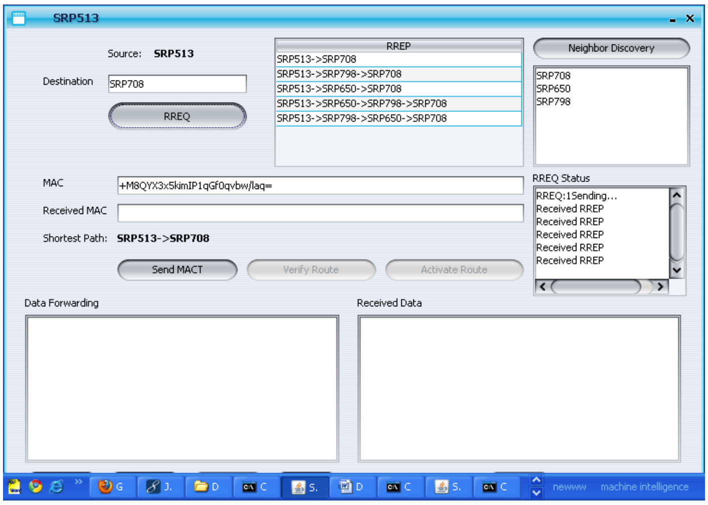
IV. IMPLEMENTATION

In this paper our scheme consists of 4 modules.

1. Nodes Creation
2. Message Authentication codes keys generation
3. Hill climbing approach
4. Multipath routing

A. Nodes Creation:

Every node can be generating at the distance specification process. Particular distance specification process to work on the transmission files of information to neighbor nodes processing. All the neighbor nodes contain that same files of information. This process is shown in Fig 4 shows the nodes creation.



Source: SRP513

Destination SRP708

RREP

SRP513->SRP708
SRP513->SRP798->SRP708
SRP513->SRP650->SRP708
SRP513->SRP650->SRP798->SRP708
SRP513->SRP798->SRP650->SRP708

SRP708
SRP650
SRP798

MAC +M8QYX3x5kimIP1qGf0qvbw/laq=

Received MAC

Shortest Path: SRP513->SRP708

RREQ Status

RREQ:1Sending...
Received RREP
Received RREP
Received RREP
Received RREP
Received RREP

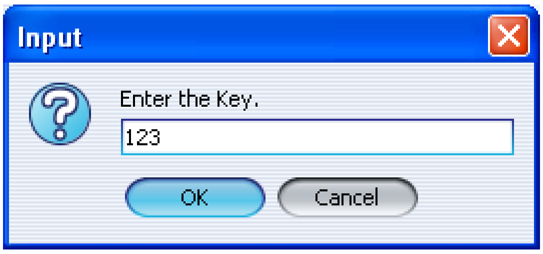
Data Forwarding

Received Data

Fig 4 existing nodes in the network

B. Message authentication code keys generation:

Every node can be working as a authentication node. Every node contains that the information like PKI. Whenever to maintain the communication all nodes can be working as a cooperation nodes. Through cooperation nodes to generate the network like cooperation network creation-process. Fig 5 shows this approach.



Enter the Key.

123

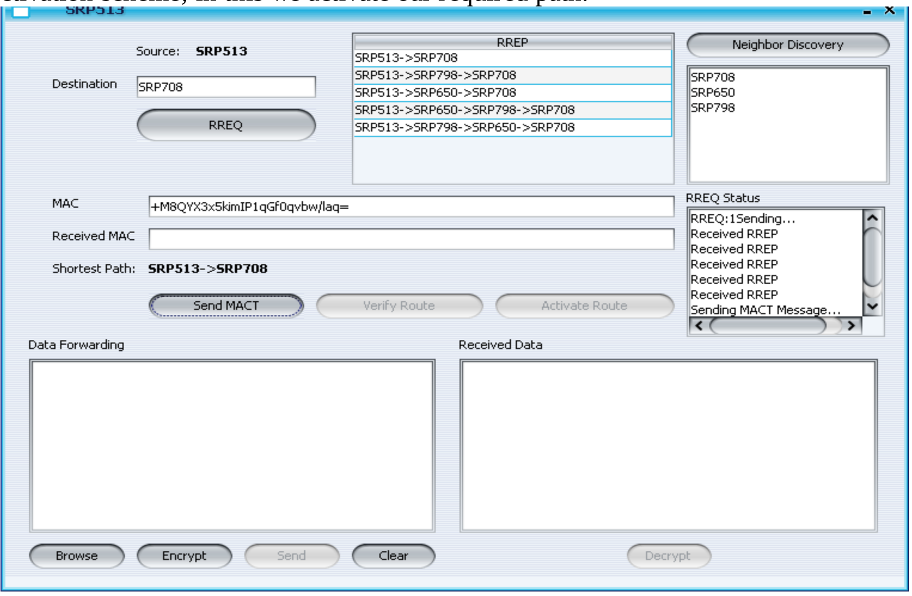
Fig 5 Enter key

C. Hill climbing approach:

The authentication keys of each node are created from a hash chain. Before sending reports, nodes disseminate their keys to forwarding nodes using Hill Climbing approach. We design the Hill Climbing approach for key dissemination, which ensures that the nodes closer to clusters hold more authentication keys than those closer to the base station do. This approach not only balances memory requirement among nodes, but also makes false reports dropped as early as possible.

D. Multipath routing:

Multipath routing is adopted when disseminating keys to forwarding nodes, which not only reduces the cost for updating keys in highly dynamic sensor networks, but also mitigates the impact of selective forwarding attacks. Fig 6 shows the path activation scheme; in this we activate our required path.



Source: SRP513

Destination SRP708

RREP

SRP513->SRP708
SRP513->SRP798->SRP708
SRP513->SRP650->SRP708
SRP513->SRP650->SRP798->SRP708
SRP513->SRP798->SRP650->SRP708

SRP708
SRP650
SRP798

MAC +M8QYX3x5kimIP1qGf0qvbw/laq=

Received MAC

Shortest Path: SRP513->SRP708

RREQ Status

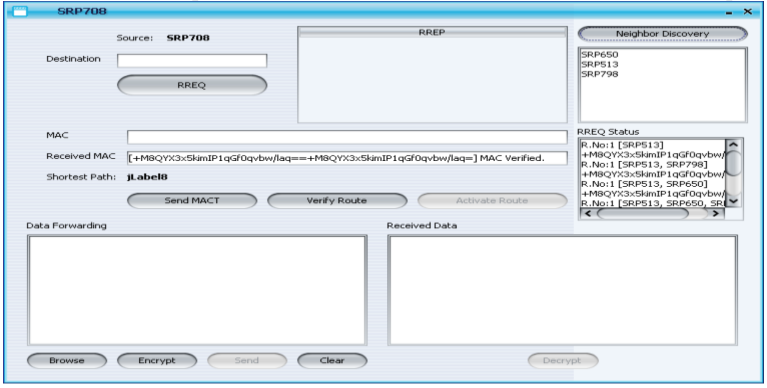
RREQ:1Sending...
Received RREP
Received RREP
Received RREP
Received RREP
Received RREP
Sending MACT Message...

Data Forwarding

Received Data

Fig 6 Request for Path Activation

Fig 7 shows the Source and path verification in this we have to verify chosen whether it is perfect or not. Fig 8 shows the path activation. In this based on previous verification we will activate user chosen path.



Source: SRP708

Destination

SRP650
SRP513
SRP798

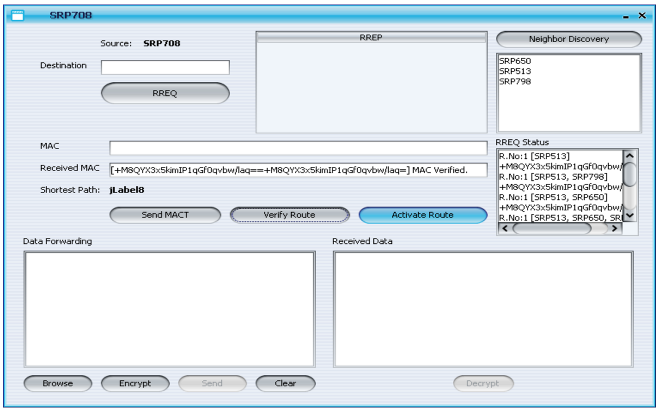
MAC

Received MAC [+M8QYX3x5kimIP1qGf0qvbw/laq==+M8QYX3x5kimIP1qGf0qvbw/laq=] MAC Verified.

Shortest Path: jLabel8

R.No:1 [SRP513]
+M8QYX3x5kimIP1qGf0qvbw/
R.No:1 [SRP513, SRP798]
+M8QYX3x5kimIP1qGf0qvbw/
R.No:1 [SRP513, SRP650]
+M8QYX3x5kimIP1qGf0qvbw/
R.No:1 [SRP513, SRP650, SR

Fig 7 Source and path verification



Source: SRP708

Destination

SRP650
SRP513
SRP798

MAC

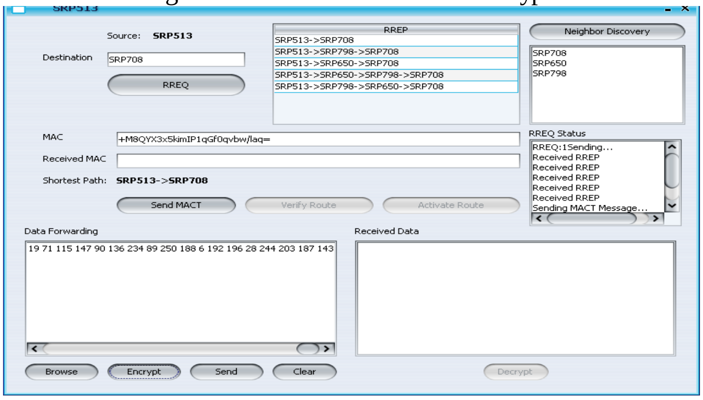
Received MAC [+M8QYX3x5kimIP1qGf0qvbw/laq==+M8QYX3x5kimIP1qGf0qvbw/laq=] MAC Verified.

Shortest Path: jLabel8

R.No:1 [SRP513]
+M8QYX3x5kimIP1qGf0qvbw/
R.No:1 [SRP513, SRP798]
+M8QYX3x5kimIP1qGf0qvbw/
R.No:1 [SRP513, SRP650]
+M8QYX3x5kimIP1qGf0qvbw/
R.No:1 [SRP513, SRP650, SR

Fig 8 Path activation

Fig 9 and 10 shows encryption and decryption of the data that mean we have to transmit the data securely. In this encryption scheme we have to use SHA algorithm and same as for the decryption also



Source: SRP513

Destination SRP708

SRP513->SRP708
SRP513->SRP798->SRP708
SRP513->SRP650->SRP708
SRP513->SRP650->SRP798->SRP708
SRP513->SRP798->SRP650->SRP708

SRP708
SRP650
SRP798

MAC +M8QYX3x5kimIP1qGf0qvbw/laq=

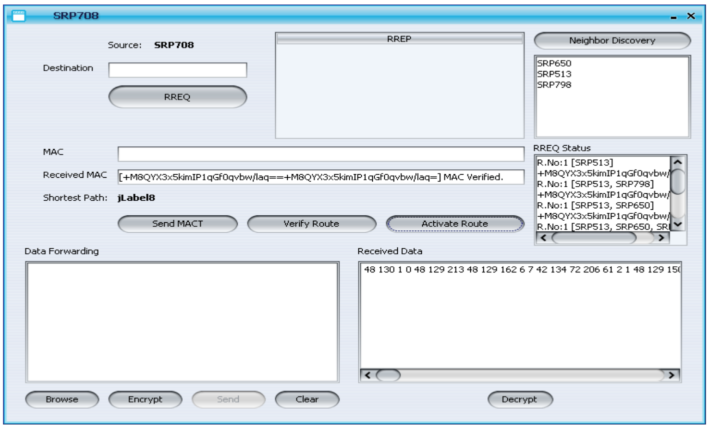
Received MAC

Shortest Path: SRP513->SRP708

RREQ:1Sending...
Received RREP
Received RREP
Received RREP
Received RREP
Received RREP
Sending MACT Message...

19 71 115 147 90 136 234 89 250 188 6 192 196 28 244 203 187 143

Fig 9 Data encoding scheme



Source: SRP708

Destination

SRP650
SRP513
SRP798

MAC

Received MAC [+M8QYX3x5kimIP1qGf0qvbw/laq==+M8QYX3x5kimIP1qGf0qvbw/laq=] MAC Verified.

Shortest Path: jLabel8

R.No:1 [SRP513]
+M8QYX3x5kimIP1qGf0qvbw/
R.No:1 [SRP513, SRP798]
+M8QYX3x5kimIP1qGf0qvbw/
R.No:1 [SRP513, SRP650]
+M8QYX3x5kimIP1qGf0qvbw/
R.No:1 [SRP513, SRP650, SR

48 130 1 0 48 129 213 48 129 162 6 7 42 134 72 206 61 2 1 48 129 15(

Fig 10 Data Decoding scheme

In summary, simulation results show that our scheme has the following advantages when compared with others:

- Our scheme drops false reports earlier even with a lower memory requirement. In some scenario, it can drop false reports in 6 hops with only 25 keys stored in each node, but another scheme needs 12 hops even with 50 keys stored.
- 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.
- *Hill Climbing* increases the filtering capacity of our scheme greatly and balances the memory requirement among sensor nodes.

V. CONCLUSIONS

Large-scale sensor networks may be deployed in a potentially adverse or even hostile environment. Due to the unattended operations of the network and the relatively small sizes of the sensors, sensor nodes may have a high risk of being captured and compromised. Instead of relying on, and complementing the efforts of, tampering prevention, in this paper, we focused on detecting false sensing reports that can be injected by compromised nodes. 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, they inform the next-hop nodes to either drop or keep on forwarding the reports.

REFERENCES

[1]. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, –A survey on sensor networks‖, *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, August 2002.

[2]. 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.

[3]. K. Ren, W. Lou, and Y. Zhang, –LEDS: Providing location-aware end-to-end data security in wireless sensor networks,‖ in *Proc. IEEE INFOCOM*, 2006, pp.1–12.

[4]. H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh,–Toward resilient security in wireless sensor networks,‖ in *Proc. ACM MobiHoc*, 2005, pp. 34–45.

[5]. 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.

[6]. H. Yang and S. Lu, –Commutative cipher based en-route filtering in wireless sensor networks,‖ in *Proc. IEEE VTC*, 2004, vol. 2, pp. 1223–1227. [7]. A.Woo, T. Tong, and D. Culler, –Taming the underlying challenges of reliable multihop routing in sensor networks,‖ in *Proc. ACM SenSys*, 2003, pp. 14–27.

[8]. –TinyOS community forum,‖ [Online]. Available: http://www.tinyos.net

[9]. Y. Yu, R. Govindan, and D. Estrin, –Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks,‖ Comput. Sci. Dept., Univ. California, Los Angeles, UCLA-CSD TR-01–0023, 2001.

10]. B. Karp and H. T. Kung, –GPSR: Greedy perimeter stateless routing for wireless networks,‖ in *Proc. ACM MobiCom*, 2000, pp. 243–254.

[11]. D. Braginsky and D. Estrin, –Rumor routing algorithm for sensor networks in *Proc. WSNA*, 2002, pp. 22–31.