A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks

Bharadwaj Iyer, Rutwij Ajgaonkar, Namita Korgaonkar, Shreyas Snehi
Mrs. Renuka Nagpure (Guide)

IT Department, Mumbai University
Atharva College of Engineering, Malad, Mumbai, India.

bharadwaj.iyer@gmail.com
rutwij15@gmail.com
namita081992@gmail.com
shreyas.snehi30@gmail.com

ABSTRACT

In wireless sensor networks, adversaries can inject false data reports via compromised nodes and launch DoS attacks against legitimate reports. In recent history, a variety of filtering schemes against false reports have been proposed. But, they either do not provide strong filtering capacity or cannot support highly dynamic sensor networks very well. Moreover, few of them are able to deal with DoS attacks at the same time. Here in this paper, we propose a dynamic en-route filtering scheme that addresses both false report injection and DoS attacks in wireless sensor networks. In our system, each node is provided with a hash chain of authentication keys used to endorse reports; meanwhile, few numbers of nodes should authenticate the legitimate report.

First, each node disseminates its key to forwarding nodes. Then, the sending nodes disclose their keys after the reports are being sent, allowing their reports to be verified by forwarding nodes. We plan the Hill Climbing key dissemination approach that ensures the nodes closer to data sources have stronger filtering capacity. We also utilize the broadcast property of wireless communication to defeat DoS attacks and adopt multipath routing to deal with the topology changes of sensor networks. If compare simulation results to existing solutions, it shows that, false reports can be dropped earlier with a lower memory necessity, especially in highly dynamic sensor networks by our designed scheme.

Keywords---Data Reporting, En-Route Filtering Scheme, Wireless Sensor Networks.

I. INTRODUCTION

In this paper, we propose a dynamic en-route filtering scheme to address both false report injection attacks and DoS attacks in wireless sensor networks. In this scheme, we organize sensor nodes into clusters(groups of nodes). Each legitimate report should be validated by multiple message authentication codes (MACs), which are produced by sensing nodes using their own authentication keys. The Hash Chain is used to create authentication keys of each node. Using Hill Climbing approach, nodes disseminate the keys to the forwarding nodes and then send the reports round-wise. In each round, every sensing node uses a new key to endorse the reports and then discloses the key to forwarding nodes. The validity of the reports is checked by the forwarding nodes with the help of the disseminated as well as disclosed keys. In our scheme, each node can monitor its neighbours by overhearing their broadcast, which forbids the compromised nodes from tampering with the reports. This process of forwarding the reports and disclosing the keys is done by the forwarding nodes at every hop until the reports are dropped completely or they manage to reach the base station.

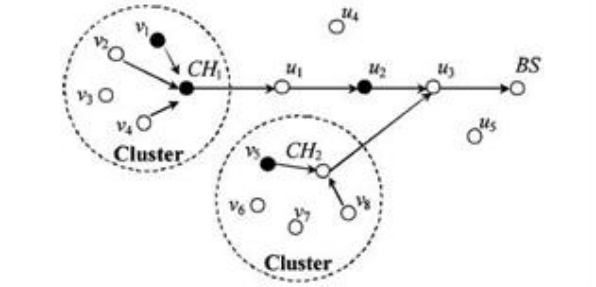

Fig. 1. Sensor nodes are organized into clusters.

Our scheme has two advantages:

• We plan 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.
• Multipath routing is adopted when disseminating keys to forwarding nodes, reducing the cost for updating keys in highly dynamic sensor networks, but also the impact of particular forwarding attacks are mitigated.

If compare simulation results to existing solutions, it shows that, false reports can be dropped earlier with a lower memory necessity, especially in highly dynamic sensor networks by our designed scheme.

Our system can be divided into three different phases:

Key pre-distribution phase, key dissemination phase, and report forwarding phase. In the key pre distribution phase, each node is loaded in advance with a distinct seed key from which it can generate a hash chain of its auth-keys. In the key dissemination phase, each node's first auth-key is disseminated by the cluster-head to the forwarding nodes, which then filter false reports. 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. Every forwarding node repeats this same process until the reports are dropped or delivered to the base station.

Our scheme is proposed to achieve the following goals:

1) To offer a stronger filtering capacity and also the ability to drop false reports earlier with an acceptable memory requirement, where we define the filtering capacity as the average number of hops travelled by a false report.

2) It can address DoS attacks or mitigate its after effects such as report disruption attacks and selective forwarding attacks.

3) It can possibly withstand highly dynamic sensor networks and should not be concerned path establishment or reparation every now and then.

4)It should not depend on fixed paths between the base station and the cluster-head for the transmission of its messages.
5) It should prevent the uncompromised nodes from being impersonated. Hence, upon detection of the compromised nodes, the clusters which are infected can easily be isolated by the base station.

Our scheme introduces new control messages and hence increases the complexity of its operations. It may suffer some attacks that are specific for itself. Here, we discuss how to deal with these attacks.

1) Attack1: A Cluster-Head is Compromised:

In our scheme, normal nodes take turns to act as the cluster-head, so there is no difference between a cluster-head and a normal node. It means that a cluster-head may be easily compromised or any compromised node can claim to be a cluster-head. A compromised cluster-head can disseminate a forged k(n) and then inject false reports arbitrarily. Our scheme offers two countermeasures to prevent this attack. First, any node including the compromised node is monitored by other nodes within the same cluster. When any node overhears a forged k(n) , it can easily detect that by checking its own auth-key that is contained in the k(n). Thus, it knows that the cluster head is compromised and can report this to the base station to revoke that node (how to revoke a node is out of the scope of
our paper).

2) Attack2: Consecutive Compromised Nodes Collaborate:

If two or more consecutive nodes are compromised and collaborate with each other, they can share the auth-keys they decrypt from to generate false reports without being monitored.

3) Attack3: Compromised Forwarding Nodes Abuses OK Message:

The OK message can be abused in either negative or positive ways. First, a compromised forwarding node can always or selectively send negative messages to make the reports dropped by its next-hop node. This is actually a selectively forwarding attack caused by the abuse of OK message. It can be addressed with the solutions we discussed above. Second, using OK message, a compromised forwarding node can cheat its next-hop node to forward false reports one more hop. Given that there are at most t-1 compromised nodes en-route, the worst case is that every two compromised nodes are separated by a uncompromised one. Therefore, in the worst case, these t-1 compromised nodes can make false reports forwarded at most 2t-2 hops.

4) Attack4: The Compromised Nodes use Invalid Node Index:

A false report containing unknown node indexes can escape from the detection of the forwarding nodes, which they thought that they do not have the corresponding auth-keys for those unknown nodes.

II. IMPLEMENTATION

In our scheme, sensor nodes are organized into clusters. Each authenticate report should be validated by multiple message authentication codes (MACs), which are produced by sensing nodes using their own authentication keys. Using a hash chain, the authentication keys are generated for each node. Using Hill Climbing approach, nodes disseminate the keys to the forwarding nodes and then send the reports round-wise. In each round, every sensing node uses a new key to endorse the reports and then discloses the key to forwarding nodes. By using the disseminated and

disclosed keys, the forwarding nodes can check the validity of the reports. In our scheme, each node can monitor its neighbors by overhearing their broadcast, thus preventing the compromised nodes to change the reports. Each forwarding node executes Report Forwarding and Key Disclosure at every hop repeatedly, up till the reports are dropped or delivered to the base station. In the proposed system false data injection is detected with secret information and it is authenticated using MAC (Message Authentication Codes). Moreover we use Hill Climbing approach to disseminate the secret keys in Sensor nodes

Now we discuss the procedure of each phase in detail.

1) Key Pre-distribution Phase:

In this phase each sensor node is loaded in advance with a unique seed key. Using the seed key, a sequence of auth-keys can be generated using a common hash function. These auth-keys, in turn, are used to encrypt the reports. The first auth-key is used first in the encryption process whereas it itself is the last key generated from the seed key. The basic assumption made over here is that the base station has full knowledge about each node's unique seed key and thus it can prevent the uncompromised nodes from being acted upon. The key pre-distribution phase is performed before the sensor nodes are deployed (e.g. it can be done in offline).

2) Key Dissemination Phase:

In our scheme, the cluster-head discloses the sensing nodes' auth-keys after sending the reports of each round. However, a malicious node can pretend to be a cluster -head and inject arbitrary reports followed by falsified auth-keys. To prevent this attack, we enforce key dissemination, that is, this phase will happen before sending the report. In this phase the cluster head aggregates the auth-keys of the sensing nodes and the cluster-head should disseminate the first auth-keys of all nodes to the forwarding nodes before sending the reports. The forwarding nodes can verify the authenticity of the disclosed auth-keys with the help of the disseminated keys, which are then used to check the validity and integrity of the reports. The first unused auth-key of a node is called the current auth-key of that node. When none of a node's auth-keys has ever been utilized, the current auth-key is nothing but the first auth-key of its hash chain.

Key dissemination should be performed periodically in case that some forwarding nodes aware of the disseminated keys become failed, especially when the network topology is highly dynamic. In this case (of re-dissemination), the first unused, instead of the first, auth-keys will be disseminated. When none of a node's auth-keys has ever been used, the present auth-key is used as the first auth-key of its hash chain.

3) Hill Climbing:

We introduce two important observations. First, when multiple clusters disseminate keys at the same time, some forwarding nodes need to store the auth-keys of different clusters. The nodes closer to the base station need to store more auth-keys than others (typically those closer to clusters) do because they are usually the hot spots and have to serve more clusters. For example, in Fig. 1, u3 serves two clusters and u1serves only one, so u3 has to store more auth-keys. Second, the false reports are mainly filtered by the nodes closer to clusters, while most nodes closer to the base station have no chance to use the auth-keys they stored for filtering. If we could let the nodes closer to clusters hold more auth -keys, the false reports can be dropped earlier. Therefore, to balance the memory requirement of nodes and provide a higher filtering capacity, we propose Hill Climbing approach, which achieves that the nodes closer to clusters hold more auth-keys than those closer to the base station do. Hill Climbing involves two variations, one for the key pre-distribution phase and the other for the key dissemination phase.

4) Report Forwarding Phase:

In this phase, sensing nodes generate sensing reports in rounds. Each round contains a fixed number of reports, e.g., 10 reports, where this number is predetermined before nodes are deployed. In each round, every sensing node chooses a new auth-key, i.e., the node's current auth-key, to authenticate its reports.

III. CONCLUSION

In this paper we have successfully implemented a dynamic en-route filtering 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 first auth-key of every node is disseminated by the cluster-head to forwarding nodes and then sends the reports followed by disclosed auth-keys. The authenticity is verified by the forwarding nodes of the disclosed keys by hashing the disseminated keys and then checks the integrity and validity of the reports using the disclosed keys. In accordance to the verification results, they inform the next-hop nodes to drop or to keep on forwarding the reports. Each forwarding node repeats this process at every single hop.

In future, there is scope to study how to take advantage of our scheme in various energy-efficient data aggregation and dissemination protocols for wireless sensor networks.

REFERENCES

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

[2] N. Bulusu, J. Heidemann, and D. Estrin, "GPS -less low cost outdoor localization for very small devices," IEEE Personal Commun. Mag., vol. 7, no. 5, pp. 28–34, Oct. 2000.

[3] S. Capkun and J. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in Proc. IEEE INFOCOM, 2005, vol. 3, pp. 1917–1928.

[4] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in Proc. ACM CCS, 2002, pp. 41 –47.

[5] T. He, C. Huang, B. Blum, J. Stankovic, and T. Ab delzaher, "Rangefree localization schemes in large scale sensor network," in Proc. ACM MobiCom, 2003, pp. 81–95.

[6] C. karlof and D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in Proc. 1st IEEE Int.Workshop Sensor Netw. Protocols Appl., 2003, pp. 113–127.

