T-Group En-Routing Approach For Detecting And Filtering Injected False Data In Sensor Networks

M. Samanna, M.Tech [CSE], KVSR Engg College, Kurnool
K. Pavan Kumar, Asst.prof & HOD in IT, KVSR Engg College, Kurnool

Abstract

Wireless sensor networks play a vital role in sharing data among various users. While data routing within the network, some hackers are going to attach false data to destroy the network by loosing energy and some nodes. In previous technologies like SEF, LBRS there is no security, reliability and filtering effectiveness. To overcome, this paper implements Grouping-enhanced Resilient Probabilistic En-route Filtering with some advanced Grouping and filtering techniques. It includes additional multi-axis division approach. This will reduces additional node grouping overhead and improves filtering capability. Compared to the existing schemes, GRPEF significantly improves the effectiveness of the en-route filtering and can be applied to the sensor networks with mobile sinks while reserving the resiliency.

Key Terms- network security, false data, and multiaxis division.

1. Introduction

Wireless networks are deployed in an unstructured manner thus adversary captures and compromise sensor nodes. Whenever any node in the sensor network is compromised then we can easily inject false data through the compromised nodes, as the result they send false reports to the base stations. These schemes implements general en-route filtering framework to protect data authenticity, detect and filter out false reports. This framework assumes that an event can be detected by more than T sensors. To protect the report authenticity, a legitimate report is collaboratively endorsed with T distinct Message Authentication Codes from the nodes detecting the event simultaneously. To filter the false reports, the nodes in the routing path share the authentication keys for the report endorsement. When an invalid report that has incorrect MAC can be detected and dropped by the forwarding nodes or the sinks. There are two ways to share the authentication keys for the report endorsement, that are, routing-specific way and probabilistic way.

In previous techniques such as IHA and LEDS, the authentication keys of sensor nodes are shared with the forwarding nodes in the routing path by pair wise key establishment or key dissemination. Since the probabilistic key sharing schemes do not need periodic node association and key dissemination, they are superior to the routing-specific key sharing schemes and are preferred by the resource-constrained WSNs. However, the existing probabilistic schemes have their shortages. In a large-scale sensor network individual sensors are subject to security compromises. A compromised node can be used to inject bogus sensing reports.

Node compromise poses severe security threats in wireless sensor networks. In existing security designs can address only a small, fixed threshold number of compromised nodes; the security protection completely breaks down when the threshold is exceeded. In this project, to overcome the threshold limitation and achieve resiliency against an increasing number of compromised nodes. To implement this draw back we propose a novel location-based approach in which the secret keys are bound to geographic locations, and each node stores a few keys based on its own location. The location-binding property constrains the scope for which individual keys can be misused, thus limiting the damages caused by a collection of compromised nodes. We illustrate this approach through the problem of report fabrication attacks, in which the compromised nodes forge non-existent events. We evaluate our design through extensive analysis, implementation and simulations, and demonstrate its graceful performance degradation in the presence of an increasing number of compromised nodes.

Routing in WSNs is very challenging due to the inherent characteristics that distinguish these networks from other wireless networks like mobile ad hoc networks or cellular networks. First, due to the relatively large number of sensor nodes, it is not possible to build a global addressing scheme for the deployment of a large number of sensor nodes as the overhead of ID maintenance is high. Thus, traditional IP-based protocols may not be applied to WSNs. In WSNs, sometimes getting the data is more important than knowing the IDs of which nodes sent the data. Second, in contrast to typical

communication networks, almost all applications of sensor networks require the sensed data from multiple sources to a particular BS. This, however, does not prevent the data to be in other forms. Third, sensor nodes are tightly constrained in terms of energy, processing, and storage capacities. Thus, they require careful resource management. Fourth, in most application scenarios, nodes in WSNs are generally stationary after deployment except for, may be, a few mobile nodes. Nodes in other traditional wireless networks are free to move, which results in unpredictable and frequent topological changes. However, in some applications, some sensor nodes may be allowed to move and change their location (although with very low mobility).Fourth, sensor networks are application specific.

Advantages

1. An efficient distributed algorithm is proposed to divide sensor nodes into exact T groups. It can guarantee that any location in the monitored area is covered simultaneously by T nodes from distinct groups with a high probability.
2. A novel location-aware key derivation technique based on multiaxis division is proposed to overcome threshold limitation of SEF.

In this we focus on the false data injection attack, in which the compromised nodes inject forged event reports to trigger false alarms or to deplete the limited resources of nodes in the routing paths. Our problem is to design a scheme that can detect and filter false reports such that false reports is detected and dropped as early as possible, the threshold limitation of the solutions is overcome, graceful performance degradation is achieved when more and more nodes are compromised, and the scheme should be independent of routing protocols and applicable to the WSNs with mobile sinks.

The mobile sink receives the data from the all nodes in network which may be false data or integrity data. After receiving data, it will identify the false inject data by en-route-filtering. When an event occurs in partition. All detecting nodes are organized into a cluster and collaboratively generate the event report E with the event location. The message authentication code of report E generated with a symmetric key. The detecting node in group computes MAC where k is the endorsement key bound with the partition. Then the detecting node sends a tuple to the cluster head CH. When CH collects MAC from distinct groups, it sends out the report with the endorsement to the sink.

En-route filtering:

- Every forwarding node verifies the MAC computed by its lower association node, and then removes that MAC from the received report.
- If the verification succeeds, it then computes and attaches a new MAC based on its pair wise key shared with its upper associated node.
- Finally, it forwards the report to the next node towards the BS.

2. Related work

First the sensor nodes are going to group into T groups, by a distributed algorithm where each node is in single group. The algorithm guarantees that every point in the terrain can be covered by sensor nodes from T distinct groups simultaneously. After the above network T-grouping, a location-aware key derivation is conducted. Then the terrain is divided into groups .Such division is called as multiaxis division.

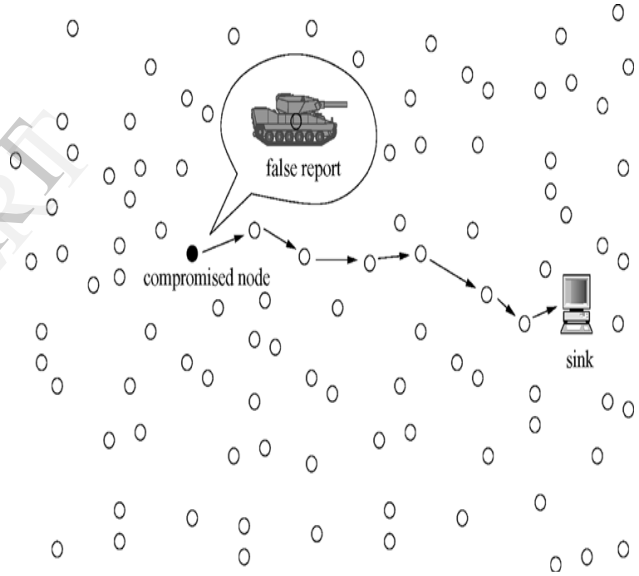

Fig: Compromised node injects false reports of nonexistent tanks" events.

GRPEF consists of the following four phases:

Pre deployment Phase: Here each node is preloaded with the value of T, the shape and size of the terrain, and the information for T-axis division.
Bootstrapping Phase: Once deployed, the WSN conducts the network T-grouping and key derivation in a short duration.
Monitoring and Reporting Phase: When an event occurs in partition, along axis, then all detecting nodes are organized into a cluster and collaboratively generate the event report E with the event location.
Then, the detecting node sends a tuple to the cluster head CH. When CH collects T MACs from distinct groups, it sends out the report.

Filtering Phase: When an forwarding node v in group gi receives an event report E, v finds the partition along axis I in which the event occurs. Then, v verifies the MAC from group gi if it holds the verification key for the partition where LE is.

Network T-Grouping:

If each group gi , is at least a 1-coverage set, then T group authentication can be carried out for events from any location in the terrain. The requirement of every group covering the whole terrain is too strict in practice, since some areas with very few sensor nodes cannot be covered by T groups. Thus, we propose a distributed network grouping algorithm DGA with the goals that each group approximately covers the whole terrain and the area exactly covered by each group is as large as possible. The algorithm DGA adopts a simple localized greedy strategy. In DGA, a virtual grid is assumed in the sensing range of each node, where l is the resolution given by users, and the sensing range of a node is defined in terms of grid points.

Location-Aware Key Derivation

In GRPEF, each node derives its endorsement keys and verification keys according to its geographic location and the group which joins. To perform the key derivation, the information is loaded to each node in the pre deployment phase: a global seed key Kg, the shape and size of the terrain, a key-sharing probability q for key derivation, the number T of groups, the angles of T axes For the location-aware key derivation, the location of a partition along axis i is represented by an integer, called as partition coordinate. Let pc be the coordinate of a partition along axis i.

3. Mechanism

Here parameter selection in GRPEF is depended on the total number of groups and the key sharing probability. Number of groups T. A bigger T makes the adversary have to compromise more sensor nodes to forge a legitimate report. However, when T increases, the size of each group will decreases in a given sensor network and so does the area covered by each group. As a result, the percentage of the area where T-group authentication can be fulfilled in the terrain, referred to as coverage percentage of T-group authentication, is reduced. Therefore, we should choose T such that it provides sufficient security strength while still enables T-group authentication for the event from almost any location in the terrain. Key sharing probability q. The key sharing probability q affects the en-route filtering effectiveness and the resiliency against node compromise. The formal results will be given in Section 5 to characterize such impact .A bigger q enables each node to share more authentication keys and thus have a higher probability to detect and drop the forged reports. However, a bigger q will also cause each node expose more keys once being compromised. Therefore, given the expected en-route filtering effectiveness, q should be as small as possible to obtain the highest possible amount of resiliency.

4. Performance Analysis

To evaluate the filtering effectiveness, we assume the adversary can use compromised keys to generate Nc correct MACs for T-group authentication of an event report. To produce a seemingly legitimate report, the adversary still has t to form groups. To compare the filtering effectiveness of GRPEF, SEF, and LBRS, we take the right side of the inequality as an estimation value. The results of the filtering probabilities of a forged report being detected and dropped within h hops in SEF and LBRS, denoted by Phse f and Ph lbrs, are given in Appendix F, available in the online supplemental material .Key Storage Overhead In GRPF, each node in group gi stores keys for the partitions intersecting with its sensing range and a few remote partitions along axis i. The key storage overhead is characterized by. Resiliency against Node Compromise According to our threat model, the adversary can combine multiple compromised keys to fabricate an event report. A combination of T keys is said to be valid if and only if the T keys are from distinct groups, and the T partitions to which these T keys are bound share a common intersection area or unit cell. By a valid combination of T keys, the adversary can forge legitimate event reports from any location in the unit cell where T partitions corresponding to these keys intersect.

Grouping Performance:

To validate the uniform property of the grouping algorithm DGA, the size of each group is investigated in the experiments. In each simulation, we ran 20,000 random tests to estimate the coverage percentage of T-group authentication after network T-grouping. In each random test, we picked a random location from the terrain and checked if there were T nodes from distinct groups in the circular area with radius Rs cantered at this location. Therefore, the simulation results conform the uniform grouping property of DGA given by Theorem we shows that the coverage percentage of GRPEF is still higher than that of SEF and LBRS even though no extra groups are used. It is because that all the nodes are grouped randomly before the node deployment in SEF and LBRS, which reduces the contribution of extra groups to the coverage degree of T group authentication, while the grouping in GRPEF is conducted after the node deployment.

5. Conclusion

In this paper the proposed GRPEF scheme is useful for en-route the false data via filtering, it was implemented by a distributed algorithm by dividing the sensor node into T groups. As a result it improves filtering effectiveness and also node compromise to achieve resiliency than previous schemes. Compared to the existing schemes, GRPEF significantly improves the effectiveness of the en-route filtering and can be applied to the sensor networks with mobile sinks while reserving the resiliency.

6. References

1. F. Ye, H. Luo, S. Lu, L. Zhang, and S. Member, "Statitical En-RouteFiltering of Injected False Data in Sensor Networks,"Proc.IEEE INFOCOM, pp. 839-850, 2004.
2. Z. Yu and Y. Guan, "A Dynamic En-Route Scheme for FilteringFalse Data Injection in Wireless Sensor Networks," Proc. IEEE INFOCOM, Apr. 2006.
3. K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-AwareEnd-to-End Data Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, Apr. 2006.
4. W. Wang, V. Srinivasan, B. Wang, and K.-C. Chua, "Coverage forTarget Localization in Wireless Sensor Networks," IPSN '06: Proc.Fifth Int'l Conf. Information Processing in Sensor Networks, pp. 118-125, 2006.

About the Authors:

N.Samanna, received his B.Tech degree in Computer Science and Engineering from Jawaharlal Nehru Technological University, Anantapur, India, in 2010. Currently pursuing M.Tech in computer science and engineering at KVSR Institute of Technology, Kurnool, India. His interesting research area is Cloud Computing, Network Security .

K.Pavan Kumar, received his B.Tech degree in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad, India. 2006; M.Tech in Computer Science from Jawaharlal Nehru Technological University, Hyderabad, India.in 2009 . He is an Asst.Professor at DR.K.V.S.R.I.T,Kurnool,A.P,India. His current research is on Mobile Ad-hoc Networks, computer networks and cloud computing.