INTERNATIONAL JOURNAL OF MERGING TECHNOLOGY AND ADVANCED RESEARCH IN COMPUTING

ISSN: 2320-1363

En-routing Approach for Tracking and injected False Data in Sensor Networks

Ankamma.K*1, Ch. Suresh*2

M.Tech (CSE) Student Department of CSE, Priyadarshini Institute of Technology & Science, Chintalapudi, Guntur(Dist), Ap, India.

Assistant Professor, Department of CSE Priyadarshini Institute of Technology & Science, Chintalapudi, Guntur(Dist), Ap, India

Abstract

Wireless Sensor Networks plays a main role in sharing data among the various users. Nodes minimize poses severe protection threats in Wireless Sensor Networks. The protection entirely breaks down when the threshold is exceeded. 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. We evaluate our design through extensive analysis, implementation and simulation its graceful performance degradation in the presence of an increasing number of compromised nodes.

Keywords: Wireless Sensor Network, Location-Based Security, Resiliency, Node Compromise, En-Route Filtering, Key Distribution.

1. Introduction

Wireless sensor networks are ideal candidates to monitor the environment in a variant of applications as military surveillance, forest fire monitoring etc. in such a network a large number of sensor nodes are deployed over a vast terrain to detect events of interest, and deliver data report over multihop wireless paths to the user. Security is essential for these mission critical applications to work in an adverse or hostile environment. One severe security threat in sensor networks is node compromise sensor nodes are typically unattended and subject to security compromise, upon which the adversary can obtain the secret keys stored I the compromised nodes and use them to launch insider attacks. This threat is aggravated as the adversary compromises more nodes and secret keys. Unfortunately most existing security design is secure against t or less compromised nodes, but completely breaks down when more than t nodes are compromised, where t is fixed threshold. In reality however there is little constraint that prevent the attacker from compromising more than the threshold number nodes.

In this paper our goal is to overcome the threshold limitation and achieve graceful performance degradation to an increasing number of compromised nodes. To this end we exploit the static and location aware nature of sensor nodes and propose a novel location based security approach through two techniques: location binary keys and location based key assignment. In this approach we bind symmetric secret keys to geographic locations, as opposed to sensor nodes, and assign such location binding keys to sensor nodes based on their deployed locations.

Our design, a Location Based Resilient Security (LBRS) solution, demonstrates that such a location based approach can effectively limit the damage caused by even a large collection of compromised nodes. In LBRS, the terrain is divided into a regular geographic grid and each cell on the grid is associated with multiple keys. Based on its location, a node stores one key for each of its local neighboring cells and few randomly chosen remote cells. Finally it limits the keys stored by individual nodes, because each node is assigned only a few keys based on its location. The result shows that LBRS is resilient, efficient, and scalable. For example in network of 4000 nodes with each node storing less than keys, LBRB can still prevent false alarms in 99% of the field.

2. Related Work

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.

Security is essential for sensor networks to work in practice in particular over adverse or hostile environments. There have been many proposals studying various aspects of sensor network security. We briefly summarize and compare the most related ones with LBRS. The key management is among the first topic explored in sensor network security. A number of pair wise key establishment schemes have been proposed. They provide basic authentication confidentiality and prevent outsiders from attacking the network. They use the idea of probabilistic key sharing to establish trust between two nodes with different emphasis on enhanced security protection flexibility of security requirements high probability of key establishment and reduced overhead or utilization of deployment knowledge. A compromised node already possesses correct keys to authenticate its message, and it can fabricate events arbitrarily. The LBRS differ from all these solutions in its capability to deal with insider attacks.

Two recent proposals SEF and IHA provide limited protection against insider attacks through probabilistic key sharing over a particular key pool and interleaved per-hop authentication, respectively. However both solutions are not resilient in that they completely lose the security protection when the attacker has compromised more than a

ISSN: 2320-1363

small fixed number of nodes. LBPS eliminates such threshold breakdown by exploiting a location based approach as the fundamental mechanism towards resilient security. To our best knowledge LBRS is the first security solution that can achieve graceful performance degradation to an increasing number of compromised nodes. The compromised nodes may launch other insider attacks than even fabrication attacks. For example they can attack the commonly used in network aggregation mechanism by producing false aggregation result. However this problem is different from event fabrication attacks in which the compromised nodes forge reports, i.e., raw data in the first place.

3. Design of LBRS

The design of our Location Based Resilient Security solution (LBRS) for report fabrication attacks. LBRS follows the general en-route filtering framework achieves resiliency against both node compromise and node failure through two novel techniques: location binary key generation and location guided key selection.

3.1Overall Operations of LBRS

As shown in Fig.3.1.1, we divide the terrain into a geographic grid and bind multiple keys to each cell on it. In that we term such keys as location binding keys. Within the key bound to one cell, each of them is associated with and identified by an index, an integer between 1 and L.

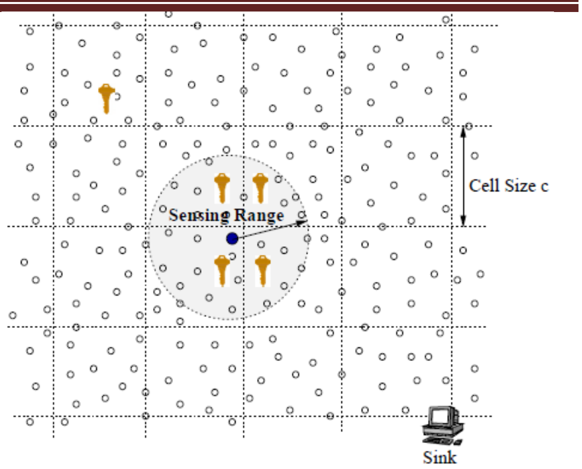


Fig.3.1.1 Each square cell on the geographic grid is associated with multiple keys. Each node stores a few local and remote cell keys based on its own location.

We assign these location binding keys to nodes based on their deployed locations. Each node stores one key for each of its sensing cells. Such keys are used to endorse events detected in those cells. Each node also stores one key for each of its verifiable cells. Such keys are used to verify events claimed to happen in those cells. A legitimate report carries m distinct MACs, jointly generated by the detecting nodes using the keys bound to the events cell. Each node then independently generates a MAC using its own key bound to the events cell, and broadcasts a tuple, where s is the key index.

Note that a legitimate node participates in report generation only when it has sensed the event by itself. Thus a compromised node cannot deceive its neighbors into endorsing a forged report. The number of MACs in a report, m, provides a tradeoff between overhead and security strength. The more MACs each report carries the stronger protection LBRS provides, yet at the cost of increased communication overhead.

The sink performs final verification on the received reports. It knows all location binding keys, thus able to verify every MAC in the report. If any of the carried MACs is incorrect the report is rejected. This is the way the sink serves as the final guard to detect and drop those forged reports that have escaped probabilistic en-route filtering.

3.2Location Binding Key Generation

The location binding approach to key generation in LBRS constraints the degree to which compromised node can abuse their keys, and minimizes the goal damage that multiple local subverted nodes can cause. To successfully forge a bogus report, the attacker must collect enough keys from a single cell, because each report must be endorsed by multiple distinct MACs using keys bound to one cell. In LBRS, in order to facilitate the generation of location-binding keys, the terrain is divided into a virtual, pre-defined geographic grid. Once a node is deployed, it obtains its own position and then derives its location-binding keys. To make this seemingly simple operation work, we need to address the following three issues:

- ✓ How to construct the grid without maintaining a real, physical infrastructure?
- ✓ How to derive keys based on the location information in a computationally efficient manner?
- ✓ How to enhance resiliency for key generation?

Constructing virtual grid: Unlike the conventional approach that maintains a real, physical grid infrastructure, we construct a virtual square grid used only to delineate cells and bind keys. Intuitively with large cells, each node can store fewer keys because there are fewer cells in total. This in turn increases the difficulty for the attacker to collect enough keys. However in this case, when the attacker has indeed obtained enough keys from one cell, he can fabricate events in larger area.

Deriving keys in an efficient fashion Before the deployment, we preload each node with the cell size C, the reference location ($X_{0,}$ Y_0) and a master secret K^I. This key derivation is efficient because it involves only local computation of light weight one way functions, without any message exchange. As a result, the bootstrapping process is very fast, and the master secret is erased before the attacker can successfully compromise any node.

Enhancing resiliency: In the above description only one key is bound to each cell. To exploit the dense sensor deployment and improve the resiliency against node compromises, we bind L distinct keys to each cell. In such cases, they contribute only one distinct MAC when a real event occurs.

ISSN: 2320-1363

4. Analysis

We analyze the performance of our design. We start with the filtering power of LBRS against single compromised node, and then analyze its resiliency when more and more nodes are compromised. We also provide an overhead analysis and a security analysis on relevant attacks. The analysis results quantify the resiliency, efficiency, and scalability of LBRS.

Simplify the analysis, we consider a circular terrain with a radius of R, over which N sensor nodes are uniformly spread at random. The sink is located at the center of the terrain, defined as the origin in the 2D coordinate space. Our analysis can be applied to other forms of terrain shapes, such as rectangles, and sink location as well.

To evaluate the filtering effectiveness, we assume the adversary can use compromised keys to generate N_c correct MAC for T-group authentication of an event report. To produce a seemingly legitimate report, the adversary still has 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.

4.1Filtering Effectiveness

We analyze the filtering performance of LBRS using two metrics:

Detection ratio: the performance of forged reports that are detected and dropped.

Filtering position: The number of hops a forged report can traverse before being dropped.

LBRS can quickly filter the forged report en-route by accumulating the filtering power along the forwarding path.

4.2Resiliency in graceful degradation

We analyze the resiliency of LBRS to an increasing number of compromised nodes. We consider a general case where the attacker compromises N nodes and fabricates report on bogus events happening in an arbitrary cell. We will show that the security protection offered by LBRS degrades gracefully, rather than completely brakes down in the entire network as in existing designs. Below we consider the worst case scenarios where all N_c compromised nodes are local neighboring nodes have largest correlation in their keys, the attacker has largest chance in compromising a cell. In addition, he may compromise a few remote cells, but LBRS limits the compromised remote cells within the upstream region of the compromised nodes.

ISSN: 2320-1363

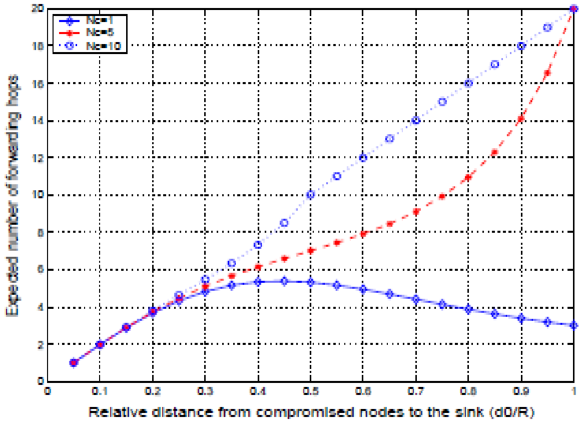


Fig 4.2.1 The performance of LBRS degrades gracefully even in the worst case scenarios.

The above graceful performance degradation in the worst-case scenarios. In this figure, we fix the node population as 4K and the terrain radius as 1KM and gradually increase $N_{c,}$ the number of compromised nodes. The figure shows that the expected number of forwarding hope for forged report increases only slightly as more nodes are compromised.

4.3Key Storage Overhead

In LBRS, each node stores one key for each sensing cell and few remote verifiable cells. The number of sensing cells is a constant, decided by the sensing range and the cell size. Thus we count only the number of keys for remote verifiable cells. Despite it's a strong filtering power, LBRS only requires the node to store a small number of keys.

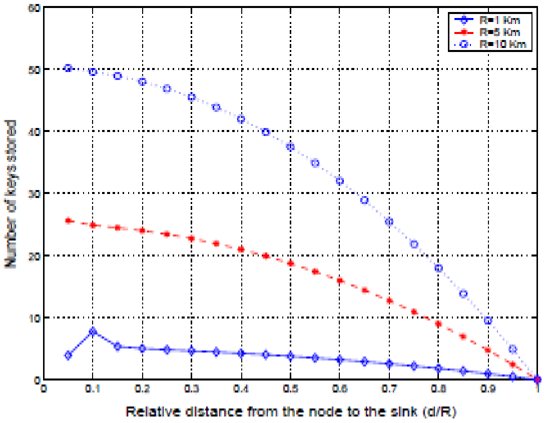


Fig 4.3.1 Each node stores only a small number of keys, and the key storage overhead scales well in large networks.

The above figure when 4K nodes are spread over a 1Km radius terrain, each node stores only 3.35keys on average, and 8keys at most. The key storage overhead is also location dependent. A node closer to the sink tends to store more keys, mainly because it has a much larger upstream region.

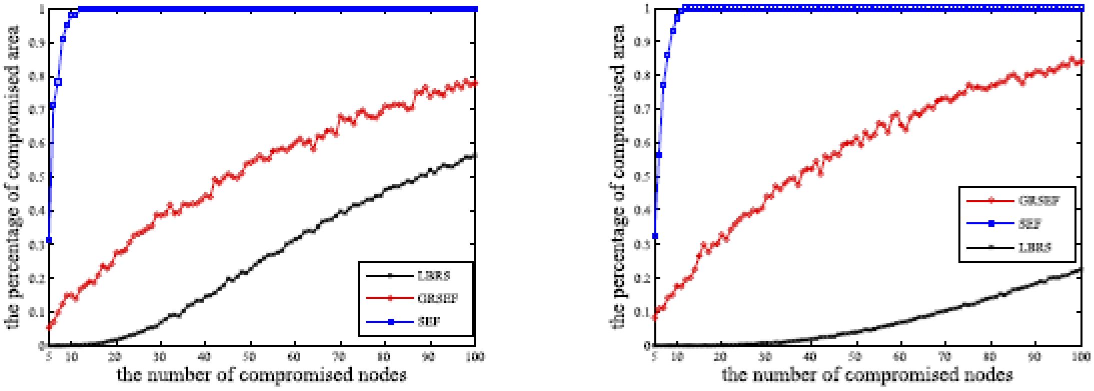
5. Simulation Evaluation

In this section we evaluate the performance of LBRS through simulation that complements our analysis. Specifically, we evaluate the resiliency of LBRS under random node compromises, and validate the beam model on geographic forwarding in the presence of node features.

Resiliency to random node compromise given that we have analyzed the worst case resiliency of LBRS when multiple compromised nodes are within the same cell, we are interested to use simulations to

ISSN: 2320-1363

study its average case performance when multiple compromised nodes are randomly distributed. For this purpose, we developed our own simulation platform using parsec, mainly because other simulators scale poorly to large number of nodes. Mainly our simulation implemented the basic geographic forwarding and the LBRS protocol stack. We simulate rectangular terrains to complement our circular terrain based analysis. Our simulation results show that LBRS is highly resilient to random node compromise.



(a) $500m \times 500m$

(b) $1000m \times 1000m$

Fig.5.1 The resiliency evaluation of GRPEF, SEF, and LBRS.

The above figure shows the percentages of the number of successes in SET, and the percentage of the compromised area of GRPEF and LBRS in two scenarios with the increasing of the number of the compromised nodes. In the figure, LBRS has a smaller percentage of compromised area than GPREF and SET is the worst. Since the beam model is adopted and each node only shares the keys of its upstream cells, LBRS requires that the sink should be static and the routing protocol must conform the beam model.

6. Conclusion

In this project node compromise presents severe security threats in sensor networks. The existing solutions either do not address such insider attacks, or completely break down when more than a fixed threshold number of nodes are compromised. As opposed to previous works, GRPEF divides sensor nodes into exact T groups to provide T group authentication by a distributed algorithm. It significantly improves the filtering effectiveness. It achieves resiliency by limiting the scope for which keys are used. Compare 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. This 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.

References

[1] R. Anderson, H. Chan, and A. Perrig. Key Infection: Smart Trust for Smart Dust. In Proc. IEEE International Conference on Network Protocols (ICNP), 2004.

[2] H. Chan, A. Perrig, and D. Song. Random Key Predistribution Schemes for Sensor Networks. In Proc. IEEE Symposium on Security and Privacy, 2003.

[3] J. Douceur. The Sybil Attack. In Proc. International Workshop on Peer-to-Peer Systems (IPTPS), 2002.

[4] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney. A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge. In Proc. IEEE INFOCOM, 2004.

[5] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, Apr. 2006.

[6] F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, "A Two-Tier Data Dissemination Model for Large-Scale Wireless Sensor Networks," Proc. ACM Mobicom, pp. 148-159, 2002.

[7] J. Albowicz, A. Chen, and L. Zhang, "Recursive Position Estimation in Sensor Networks," Proc. Ninth Int'l Conf. Network Protocols (ICNP), pp. 35-41, 2001.

[8] L. Lazos and R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks," Proc. Third ACM Workshop Wireless Security (WiSe '04), pp. 21-30, 2004.

[9] S. Capkun and J. pierre Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," Proc. IEEE INFOCOM, 2005.