International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 1; Issue: 6; October–2013

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

Mrs. S. Saritha[1] , Mr. M . Raja Sekhar[2]
[1]M.Tech. 2nd Year Dept. of CSE, [2] Asst. Professor Dept. of CSE
[1,2] Indira Priyadarshini College of Engineering. Engg.& Technology for women
Nannur Village, Orvakal Mandal ,Kurnool Dist A.P.- 518023.

Abstract: In this paper, we propose a dynamic en-route filtering scheme for false data injection attacks in wireless sensor networks. In sensor networks, adversaries can inject false data reports containing bogus sensor readings or nonexistent events from some compromised nodes. Such attacks may not only cause false alarms, but also drain out the limited energy of sensor nodes. Several existing schemes for filtering false reports either cannot deal with dynamic topology of sensor networks or have limited filtering capacity. In our scheme, a legitimate report is endorsed by multiple sensing nodes using their distinct authentication keys from one-way hash chains. Cluster head uses Hill Climbing approach to disseminate the authentication keys of sensing nodes along multiple paths toward the base station. In filtering phase, each forwarding node validates the authenticity of the reports and drops those false reports. Compared to existing schemes, our scheme can better deal with dynamic topology of sensor networks. Analytical and simulation results show that our scheme can drop false reports earlier even with a lower memory requirement and tolerate more compromised nodes. Our scheme also outperforms others in term of energy efficiency, especially for large sensor networks.

Keywords: Cluster Application, Sensor Network, Dynamic network topology .

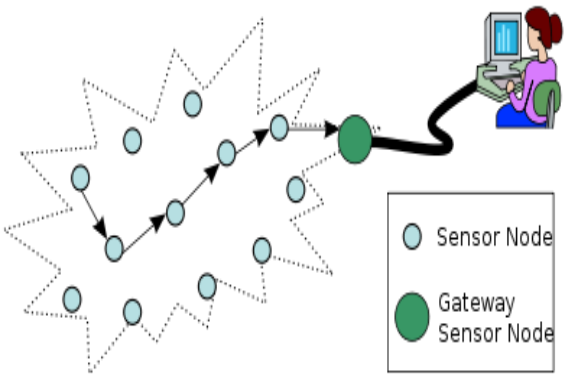
1 INTRODUCTION

WIRELESS sensor networks consist of a large number of small sensor nodes having limited computation capacity, restricted memory space, limited power resource, and short-range radio communication device. In military applications, sensor nodes may be deployed in hostile environments such as battlefields to monitor the activities of enemy forces.In these scenarios, sensor networks may suffer different types of malicious attacks. One type is called false report injection attacks , 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.

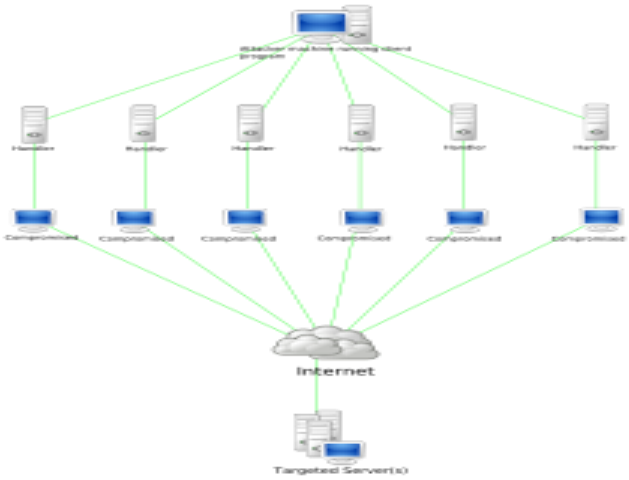
In selective forwarding attacks [12], they may selectively drop legitimate reports, while in report disruption attacks [11], they can intentionally contaminate the authentication information of legitimate reports to make them filtered out by other nodes. Therefore, it is very important to design a dynamic quarantine scheme to filter these attacks or at least mitigate their impact on wireless sensor networks. Recently, several schemes such as SEF [15], IHA [14], CCEF [13], LBRS [12], and LEDS [10] have been proposed 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[16]. IHA has a drawback, that is, it must periodically establish multi hop pair wise keys between nodes[6]. 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 [7][2]. 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 [3], [8],[9]. In LBRS, report disruption attacks are simply discussed, but no concrete solution is proposed.

We propose a dynamic en-route filtering scheme that addresses both false report injection and DoS attacks in wireless sensor networks. In our 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. First, each node disseminates its key to forwarding nodes. Then, after sending reports, the sending nodes disclose their keys, allowing the forwarding nodes to verify their reports. We design the Hill Climbing key dissemination approach that ensures the nodes closer to data sources have stronger filtering capacity. Moreover, we exploit the broadcast property of wireless communication to defeat DoS attacks[5] and adopt multipath routing to deal with the topology changes of sensor networks.



Denial-of-service attack



A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. The term is generally used relating to computer

networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.[1]

EXISTING SYSTEM

One type is called false report injection attacks, 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, they may selectively drop legitimate reports, while in report disruption attacks; they can intentionally contaminate the authentication information of legitimate reports to make them filtered out by other nodes.

PROPOSED SYSTEM

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

Module Description:

Key Pre distribution Phase:

Key pre distribution needs to be performed only once. It consists of two steps.

Step1*:* Each node is preloaded with a distinct seed key. From the seed key, it can generate a sequence of auth-keys using a common hash function[4] . Thus, each node's auth keys form a hash chain.

Step2: Among n nodes of a cluster, we assume that there are at least nodes each having a distinct -key.

Key Dissemination Phase :

In our scheme, the cluster-head discloses the sensing nodes' auth-keys after sending the reports of each round. However, it is vulnerable to such an attack that 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, the cluster-head should disseminate the first auth-keys of all nodes to the forwarding nodes before sending the reports in the first round. By using the disseminated keys, the forwarding nodes can verify the authenticity of the disclosed auth-keys, which are in turn used to check the validity and integrity of the reports.

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.. When none of a node's auth-keys

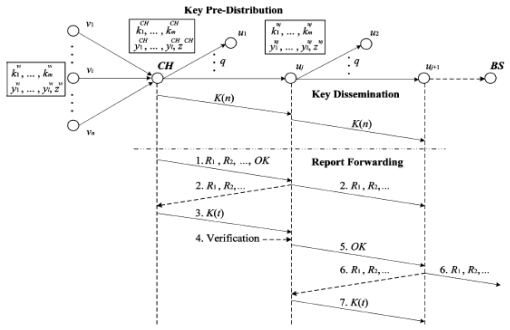
has ever been used, the current auth-key is just the first auth-key of its hash chain .

Hill Climbing 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. 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. Hill Climbing involves two variations, one for the key pre distribution phase and the other for the key dissemination phase.

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.

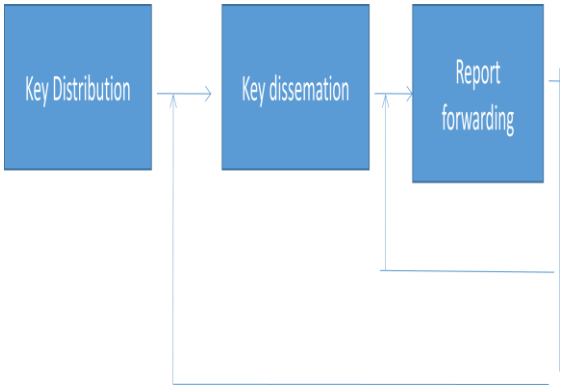
Detailed view of all three phases



Goals:

- It can offer stronger filtering capacity and drop false reports earlier with an acceptable memory requirement, where the filtering capacity is defined as the average number of hops that a false report can travel.
- It can address or mitigate the impact of DoS attacks such as report disruption attacks and selective forwarding attacks.
- It can accommodate highly dynamic sensor networks and should not issue the process of path establishment or reparation frequently.
- It should not rely on any fixed paths between the base station and cluster-heads to transmit messages.
- It should prevent the uncompromised nodes from being impersonated. Therefore, when the compromised nodes are detected, the infected clusters can be easily quarantined by the base station. delivered to the base station

The relationship between three phases:



CONCLUSION :

The entire paper has been developed and implemented as per the requirements. A dynamic en-route quarantine 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 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. This process is repeated by each forwarding node at every hop.

Future Enhancement

In future, we will study how to take advantage in our scheme of 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. Abdelzaher, "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.

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

[8] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization

forWireless sensor networks," in *Proc. ACMWiSe*, 2004, pp. 21–30.

[9] L. Lazos, R. Poovendran, and S. Capkun, "ROPE: Robust position estimation

in wireless sensor networks," in *Proc. IPSN*, 2005, pp. 324–331.

[10] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proc. ACM CCS*, 2003, pp. 52–56.

[11] A. Perrig, R. Szewczyk, V. Wen, D. Culer, and J. Tygar, "SPINS: Security

protocols for sensor networks," in *Proc. ACM MobiCom*, 2001, pp. 189–199.

[12] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation

in sensor networks," in *Proc. ACM SenSys*, 2003, pp. 255–265.

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

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

Dept., Univ. California, Los Angeles, UCLA-CSD TR-01–0023, 2001.

[15] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," in *Proc. IEEE INFOCOM* 2006, pp. 1–12.

[16] 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.