Message Authentication in Sensor Networks Using En-route Filtering

K.J. Sridevi
Department of Computer Science, St.Joseph's college of Arts and Science for Women, Hosur-635126
Email: devi.bala@rediffmail.com

----------ABSTRACT----------

In a large-scale sensor network individual sensors are subject to security compromises. A compromised node can be used to inject bogus sensing reports. If undetected, these bogus reports would be forwarded to the data collection point (i.e. the sink).such attacks by compromised nodes can result in not only false alarms but also the depletion of the finite amount of energy in a battery powered network. In this paper, we present a en-route filtering mechanism to detect and drop false reports during the forwarding process. Assuming that the same event can be detected by multiple sensors, in en-route each of the detecting sensors generates a keyed message authentication code (MAC) and multiple MACs are attached to the event report. En-route filtering exploits the network scale to filter out false reports through collective decision-making by multiple forwarding nodes. It can drop up to 70% of bogus reports injected by a compromised node within five hops, and reduce energy consumption by 65% or more in many cases.

Keywords - Compromised nodes, en-route filtering, false data injection, Denial of service attack, Group rekeying en-route filtering

---

1.INTRODUCTION-WIRELESS SENSOR NETWORK

A Wireless Sensor Network (WSN) is composed of a large number of small sensor nodes having limited computation capacity, restricted memory space, limited power resource, and short-range radio communication device. It has a base-station or sink, which does the functions of calculation and decision-making, and can be compared with the functionalities of server or in some cases as a gateway in a computer network. The nodes communicate wirelessly and often self-organize after being deployed in an ad-hoc fashion.

In this, we can have thousands of nodes, with each node performing some allocated function. Such systems can revolutionize the way we live and work. Within few years, we can expect them to cover a substantial part of the world with access to them via the internet. This can be considered as the internet becoming a physical network. This exciting technology has unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, smart spaces and many more (fig. 2).

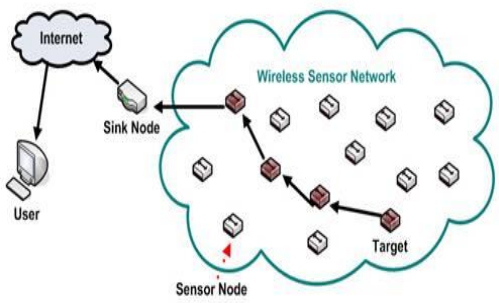

Fig. 1 A typical Wireless Sensor Network

Since WSNs are generally deployed in an unattended, hostile and adverse environment, hence the chances of threats and attacks are very high. So the design of an efficient authentication scheme is of great importance to secure the data flowing in the WSNs.

Fig. 2 A sensor Node

Sensor networks are vulnerable to many attacks and to put it in a more generalized way, they are mainly susceptible to False Data Injection attacks and Denial-of-Service attacks. Most of the attacks aim to suck out the energy of the nodes by draining the battery of the node, thereby making the node to sleep indefinitely; disrupting the communication in the sensor network (fig. 3).

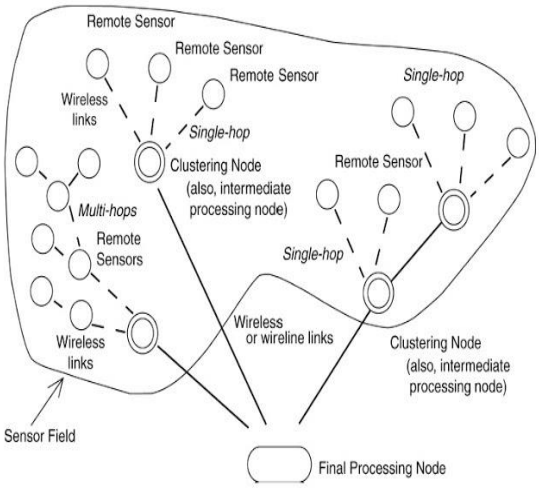

Fig 3. A Brief Description of a Sensor Network.

2. FALSE DATA INJECTION ATTACK

In this attack, the adversary injects some false data into the sensor nodes so that the objective of the sensor network, containing that node, is affected. When a sensor network is deployed in unattended and hostile environments such as battlefield, the adversary may capture and reprogram some sensor nodes into the network and make the network accept them as legitimate nodes. After getting control of a few nodes, the adversary can mount various attacks from inside the network (fig 4).

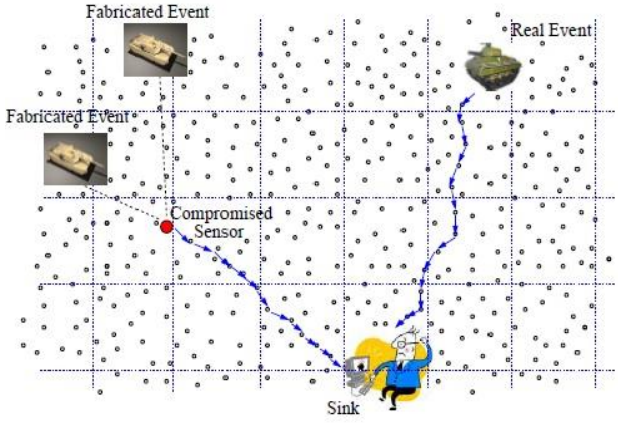

Fig 4. A compromised node will send the Message of Fabricated Events Instead of the Real Events.

3.DENIAL-OF-SERVICE (DOS) ATTACK

The three main features for security of a message traversing the network are confidentially, Integrity and Availability (CIA). Confidentially prevents unauthorized parties from accessing secure data. Integrity guarantees that data isn't modified in transit and that replayed packets aren't accepted as the original. Availability ensures that authorized parties can access data, services, or other computer and network resources when requested. DoS attacks target availability by preventing communication between network devices or by preventing a single device from sending traffic. Since the network is flooded with bogus requests of the attacker, the legitimate parties are not able to perform its tasks (Fig 6). easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

The various DoS attacks categorized according to layers are.

- Physical Layer-Jamming, Node Tampering.
- Data Link Layer-Collision, Exhaustion, Unfairness, Interrogation, Denial-of-Sleep, Jamming.
- Network Layer- Homing, Hello Floods.
- Transport Layer- TCP SYN (synchronize) Flood Attack, Desynchronization, and Session Hijacking.
- Application Layer-Deluge (reprogramming) attack, Path-based DoS (PDoS) (Fig 7).

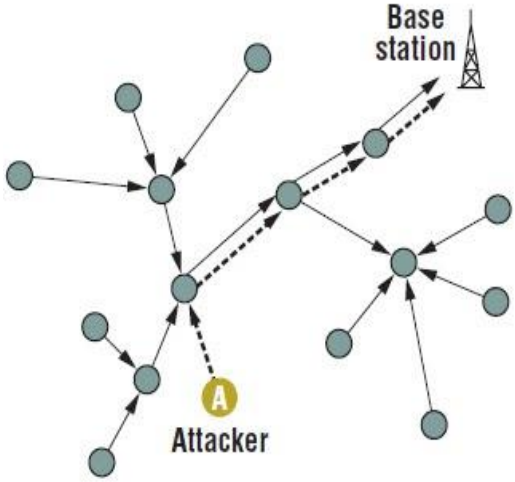

Fig 7. A Path Based DoS (PDoS) Attack.

4.EN-ROUTE FILTERING

En-route Filtering is a scheme in which not only the destination node but also the intermediate nodes can check the authenticity of the message in order to reduce the number of hops/nodes the bogus message in order to reduce the number of hops/nodes the bogus message travels. For example, there are five nodes in a network, namely, A, B, C, D, E; where A is the sender and E is the receiver, say, Base Station; and B, C and D are intermediate nodes. Suppose a bogus data injected in the path between B and C, so when this bogus message reaches C, it gets filtered out of the path. Therefore, the bogus message does not traverse D and E; thereby, conserving energy (Fig 8). At this point, some might argue that how is it energy efficient when each node has to perform authentication?. An apparent answer for this question is that practically, the sensor network consists of thousands of nodes, not 5-6 nodes and if the bogus message is filtered out in the next intermediate/filtering node itself, then hundreds or even thousands of the remaining nodes in the path of traversal of the message will be spared. A noteworthy point here is that since the sensor network consists of thousands of nodes, so the authentication/filtering process is present in selected nodes only; another important aspect for efficient use of energy.

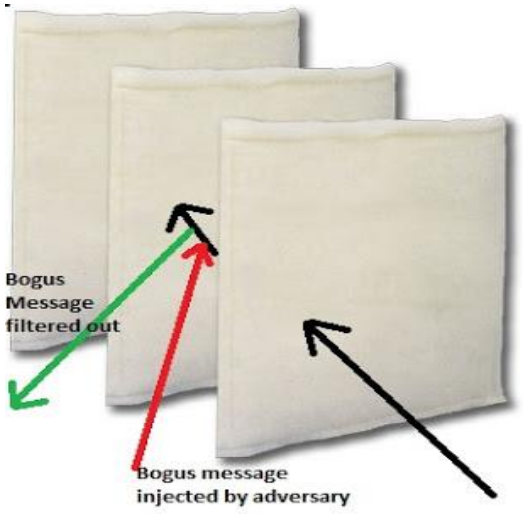

Fig 8. En-Route Filtering

En-route filtering is an effective way to mitigate the false data injection attacks and DoS attacks. As False data injection is concerned, the maliciously injected false data will be filtered out as soon as possible, that is, in the subsequent filtering node itself. So, the bogus message will not reach the other remaining nodes present on the path to the base station. Hence, the remaining nodes will be spared any procedures, thereby, saving energy.

As DoS is concerned, it is more or less a resultant of the false data injection attack. When too many nodes are compromised due to false data injection, then the bogus message will pass through many nodes, thereby creating a jam in the network. To mitigate this, En-route Filtering is an Effective procedure since the bogus chain will be filtered out in its early stages so that the legitimate parties can use the network effectively.

5.WORKING OF EN-ROUTE FILTERING

There are many ways to perform this scheme. Some of them are: Dynamic (active), Statistical, Commutative, Cipher-based, Constrained function-based, Priority-based, Group rekeying-based, Secure ticket-based and few more. The following part of the composition will cover some of these before-mentioned schemes (Fig 9).

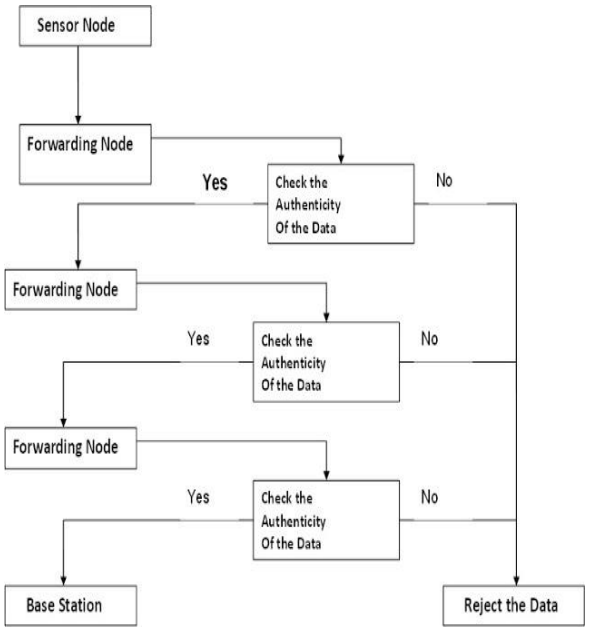

Fig 9. The Activity Diagram of En-Route Filtering Scheme

5.1 Statistical En-route Filtering:

This scheme takes advantage of the large-scale and dense deployment of sensor networks. Its detection and filtering power increases with the deployment density and the sensor field size. It can be effectively detect false reports even when the attacker has obtained the security keys from a number of compromised nodes, as long as those keys belong to a small number of the key pool partitions. It can filter out 80-90% false data by compromised nodes. To prevent any single compromised node from breaking down the entire system, this scheme carefully limits the amount of security information assigned to any single node, and relies on the collective decisions of multiple sensors for false report detection. When an event occurs in the field, multiple surrounding sensors collectively generate a legitimate report that carries multiple Message Authentication Codes (MACs).

A report with an in adequate number of MACs will not be delivered. As a sensing report is forwarded towards the sink over multiple hops, each forwarding node verifies the correctness of the MACs carried in the report with certain probability. Once an incorrect MAC is detected, the report is dropped. The probability of detecting incorrect MACs increases with the number of hops the report travels. Depending on the path length, there is a non-zero probability that some reports with incorrect MACs may escape en-route filtering and be delivered to the sink. In any case, the sink will further verify the correctness of each MAC carried in each report and reject false ones. Collaborative filtering of false reports requires that nodes share certain amount of security information. The more security information each forwarding node possesses, the more effective the en-route filtering can be, but the con is that if somehow more number of nodes is compromised, then the attacker can obtain more secret from a compromised node.

5.2Secure Ticket-Based En-Route Filtering

This scheme addresses false data injection and PDoS attack in sensor networks. This is a lightweight ticket concept which is applicable in resource constrained WSNs. Messages to the sink are only valid if they contain a valid ticket. Each en-route node which forwards a message is able to verify the validity of the ticket and drops the message if the ticket is invalid. Hence, a false message can be filtered out immediately. The ticket concept enables the separation of report generation with sink verification, and the en-route filtering, without the need for symmetric key sharing between sensor nodes. This results in a high resiliency against node compromise. Even if an adversary compromises several nodes, he is not able to inject as many messages as desired to perform a successful PDoS attack because he does not possess the necessary tickets. If a region is under suspicion to be compromised it can be easily excluded by simply not sending query messages containing valid tickets there.

Moreover, node compromises are limited to the immediate vicinity of the compromised nodes and do not affect the whole network. Taking performance into consideration, this scheme is able to significantly reduce the energy consumption by immediate filtering of false reports. Its energy savings increase with the number of injected false messages and with the distance to the sink where an adversary injects false messages. Furthermore, the storage requirements in the sensor nodes is very low, and thus, it is applicable in high density networks, and leaves room for further security mechanisms, that can add to the concept of defence-in-depth for the sensor network.

5.3Group Rekeying-Based En-Route Filtering

It is basically a family of Pre distribution and local Collaboration-based Group Rekeying (PCGR) schemes to address the node compromise problem and to improve the effectiveness of filtering false data in sensor networks. These Schemes are based on the idea that future group keys can be preloaded before deployment, and neighbours can collaborate to protect and appropriately use the preloaded keys. It can achieve a good level of security, outperform most existing schemes, and significantly improve the effectiveness of filtering false data. In addition to filtering false data, these schemes can also be applied to other group rekeying problems, especially for scenarios where a group has a large number of widely spread members, the membership changes frequently, or when it is very expensive to maintain a central key manager.

5.4Priority-Based En-Route Filtering

This scheme is primarily based on the concept of votes and the network is divided into clusters, and it aims to control the number of votes. It determines priorities through the fuzzy rule-based system. Each cluster-head receives priority from the base station and the cluster-head attaches a specified number of votes to the report according to the priority.

In this scheme, each verification node will check on the vote that is generated by nodes in the same cluster. If it is true, then the event report will be passed, otherwise it will be dropped. It will be dropped. It will then verify a vote using the corresponding verification key. The node will check that the number of the false reports or the number of the true votes among the verified votes has reached the threshold. There is an adaptive security threshold value, which is the output of the fuzzy-rule based system, which in turn plays a vital role in enhancing the capability of this scheme. It determines the trade-off between the security level and the amount of energy consumed.

This scheme uses the rate of false reports rejected by the base station, the frequency of event reports and the estimated distance from the base station to cluster as inputs to the fuzzy rule-based system to determine the security through the fuzzy rule based system.

5.5Commutative Cipher-Based En-Route Filtering

This scheme differs from existing security solutions in that it decouples base station verification from en-route filtering, and does not share any symmetric keys between the sensors nodes. It exploits the typical operational mode of query response in sensor networks, and installs security states in the nodes in an on-demand manner, and is preloaded with a unique node key. The base station initiates a query response session by sending out a query to task specific sensor nodes to report their sensing results. The base station prepares two keys for each session: one session key and one witness key.

The session key is securely sent to source node, i.e., the node tasked to generate reports, while the witness key is in plaintext and recorded by all intermediate nodes. A legitimate report is endorsed by a node MAC jointly generated by the detecting nodes using their node keys, and a session MAC generated by the source node using the session key. Through the usage of a commutative cipher, a forwarding node can use the witness key to verify the session key, and drop the fabricated reports. The base station further verifies the node MAC in the report that it receives, and refreshes the session key upon detection of compromised nodes. It can provide much stronger security protection against compromised nodes than the symmetric key sharing based designs.

5.6Dynamic (active) En-Route Filtering

In this scheme, each node uses its own authentication-keys to authenticate their reports and a legitimate report is endorsed by nodes. The authentication-keys of each node form a hash chain and are updated in each round. The cluster-head disseminates the first authentication-key of every node to forwarding nodes and then sends the reports followed by disclosed authentication-keys. The forwarding nodes verify the authenticity of 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.

There are several advantages of this scheme. This scheme can drop false reports much earlier even with a smaller size of memory. The uncompromised nodes will not be impersonated because each node has its own authentication-keys. Therefore, once the compromised nodes are detected,

the infected clusters can be easily quarantined. This approach increases filtering capacity greatly and balances the memory requirement among nodes. This scheme is adaptive to highly dynamic networks and also mitigates the impact of selective forwarding attacks. Monitored by its upstream nodes and neighbours, the compromised nodes have no way to contaminate legitimate reports or generate false control messages.

However, for all these above-mentioned advantages, there are some trade-offs. This scheme is more complicated than the Statistical En-route Filtering scheme due to introduction of some extra control messages. The use of these control messages not only increases operation complexity, but also incurs some extra overhead. The introduction of extra control messages triples the delay of reports. Here, each node uses the same authentication-key to authenticate all of its reports in the same round. Therefore, this authentication-key can only be disclosed after the forwarding nodes forward the reports to their next-hop nodes, which increases memory overhead of the forwarding nodes. This scheme cannot be easily coordinated with other energy-efficient protocols, because in this scheme each node has to be awake until it overhears the broadcast of its next-hop node.

5.7Constrained Function-Based En-Route Filtering

In this scheme, the current aggregator concept is used. This aggregated is selected on the basis of attributes of nodes, and it gathers and stores the information from its neighboring nodes in order to perform certain computational procedures. Hash function is employed to generate MACs, used to endorse the sensor readings so that each intermediate node can verify the authenticity of forwarding messages.

It exhibits: *Resilience to node compromise*, which means that the compromised nodes cannot forge the messages sent from the genuine nodes; *independence of network settings*, which means that this scheme has low computational and communication overhead. With these characteristics, this scheme is constructed in such a way that the source node sends a message to the destination node, together with the corresponding constrained function based endorsements generated by the neighbouring nodes. Afterwards, the source node can determine if the neighbouring nodes has send the false endorsement and each intermediate node has the ability to check the authencity of forwarding messages.

6.CONCLUSION

The world is changing fast from wired networks, to wireless networks, and now to wireless sensor networks. In this composition, the present and future scenario of wireless sensor networks was stated, which shows its unlimited potential. Due to this high importance, it is susceptible to various attacks, mainly false data injection attacks and Denial-of-Service attacks. At this point, En-route Filtering comes into picture since it is an efficient way of dealing with these attacks. Instead of filtering the message only at the destination node or sink, En-Route Filtering scheme filters the unauthentic message at the next forwarding node itself. So, it spares the remaining nodes in the path from any computational procedures, thereby conserving energy. Furthermore, different En-Route Filtering schemes were stated. Each of these schemes has its own pros and cons. So, it is up to the certain specific requirement of the users and organizations which scheme is required to be used by them.

REFERENCES

[1] V. Wen, A. Perrig, and R. Szewczyk, “SPINS: Security suite for sensor networks,” in Proc. ACM MobiCom, 2001, pp. 189–199.

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

[3] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in Proc. IEEE Symp. Security. Privacy,May 2003,pp. 197–213.

[4] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, “URSA: Ubiquitous and robust access control for mobile ad hoc networks,” Proc. IEEE/ACM Trans. Netw., vol. 12, no. 6, pp. 1049–1063, Oct. 2004, to be published.

[5] K. Park and H. Lee, “On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets,” in Proc. ACM SIGCOMM, 2001, pp. 15–26.

[6] S. Basagni, K. Herrin, E. Rosti, and D. Bruschi, “Secure pebblenets,” in Proc. ACM MOBIHOC, 2001, pp. 156–163.

[7] D.W. Carman, P. S. Kruus, and B. J. Matt, “Constraints and approaches for distributed sensor network security,” NAI Laboratories, Tech. Rep. 00–010, 2000.

[8] F. Ye, G. Zhong, S. Lu, and L. Zhang, “GRAdient broadcast: A robust data delivery protocol for large scale sensor networks,” ACM Wireless Netw. (WINET), vol. 11, no. 2, Mar. 2005.

[9] M. Bellare, R. Canetti, and H. Krawczyk, “Keying hash functions for message authentication,” Proc. Crypto, pp. 1–15, 1996.

[10] TinyOS Operation System [Online]. Available: http://millennium. berkeley.edu