IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 6 (Jul. - Aug. 2013), PP 29-31
www.iosrjournals.org

Filtering Schemes for Injected False Data in Wsn

Shahina K[1], Anand Pavithran[2]
[1, 2](Department Of Computer Science and Engineering, India)

Abstract: *Wireless sensor networking is an emerging technology, which supports many emerging applications due to their low cost, small size and unethered communication over short distances. Sensor nodes are deployed in open hostile environment in WSN applications. An adversary can easily compromise sensor nodes due to their unattended nature. Adversaries can inject false data reports into the WSN through compromised nodes. The false data reports lead the en-route nodes and the base station to make false decision. False decision depletes the energy of en-route nodes and the base station. Hence create threat to the lifetime of the sensor nodes. To detect and drop false data, number of en-route filtering schemes have been developed. Bandwidth Efficient Cooperative Authentication scheme for injected false data(BECAN) is an efficient method for filtering false data. Here, implements the BECAN scheme by using NS2 and increases the security by adding Hybrid Authentication scheme (HAS).*

Keywords: *En-route filtering, Sensor node, false data.*

I. Introduction

In WSN applications sensor nodes are deployed in hostile environment. In such environment sensor nodes are subjected to various types of attacks such as eavesdropping, masquerade, false data injection, selective forwarding. Sensor nodes sense the events and generate event report for the sensed information and the event report has to be send to the base station through the en-route nodes. When event report is forwarded through en-route node, a compromised node can forge the report. False data contain false information from compromised nodes. The false data injection attack depletes the energy of the en-route nodes. One solution to reduce the impact of false data injection into the network through a compromised node is to filter the false data by the en-route node as early as possible before reaching the base station. Many enroute filtring schemes have been developed. Statistical en-route filtering is the first en-route filtering scheme (SEF) [1] to address the fabricated Report injection attacks in the presence of compromised nodes. Commutative Cipher based En-route Filtering scheme (CCEF)[2] drops fabricated reports en-route without symmetric key sharing. In Secure Ticket-Based Enroute Filtering Scheme (STEF)[3], ticket concept is introduced to drops false messages enroute. Dynamic En-route Filtering [4] is based on clustering. Finally BECAN [5] is band-width efficient co-operative authentication scheme for filtering injected false data.

II. Literature Survey

2.1 Sef

Statistical en-route filtering (SEF)[1] is the first en-route filtering scheme to address the fabricated report injection attacks in the presence of compromised nodes and introduce an en-route filtering framework. In SEF, there is a global key pool, which is divided into n non-overlapping partitions. Before deployment, each node stores a small number of authentication keys randomly selected from one partition of globe key pool.Once a stimulus appears in the field, multiple detecting nodes elect a CoS node that generates the report. Each detecting sensor produces a keyed MAC for the report using one of its stored keys.The CoS node collects the MACs and attaches them to the report in the form of a Bloom filter. These multiple MACs collectively act as the proof that a report is legitimate. A report with insufficient number of MACs will not be forwarded. When sink receives reports about an event, the sink verifies every MAC because it knows all the keys. Thus false reports with incorrect MACs that sneak through enroute filtering by chance are still detected. SEF cannot detect which nodes are compromised because reports are filtered en-route probabilistically, but it can prevent the false data injection attack with 80 - 90 percent probability within 10 hops.

2.2 Ccef

In Commutative Cipher Based En-route Filtering (CCEF)[2], each node is preloaded with a distinct authentication key. When a report is needed, the base station sends a session key to the cluster-head and a witness key to every forwarding node along the path from itself to the cluster-head. The report is appended with multiple MACs generated by sensing nodes and the cluster-head. When the report is delivered to the base station along the same path, each forwarding node can verify the cluster-heads MAC using the witness key. The MACs generated by sensing nodes can be verified by the base station only. CCEF has several drawbacks. First, it relies

on fixed paths as IHA does. Second, it needs expensive public key operations to implement commutative ciphers. Third, it can only filter the false reports generated by a malicious node without the session key.

2.3 Stef

Secure Ticket-Based En-route Filtering (STEF) [3],uses a ticket concept, where tickets are issued by the sink and packets are only forwarded if they contain a valid ticket. If a packet does not contain a valid ticket, it is immediately filtered out. STEF is similar nature to SEF and DEF[4]. The packets contain a MAC and cluster heads share keys with their immediate source sensor nodes in their vicinity and with the sink. The drawbacks of STEF are its one way communication in the downstream for the ticket traversal to the cluster head.

2.4 Def

In Dynamic En-route Filtering scheme (DEF) scheme, a legitimate report is endorsed by multiple sensing nodes using their own authentication keys. Before deployment, each node is preloaded with a seed authentication key and secret keys randomly chosen from a global key pool. Before sending re-ports, the cluster head disseminates the authentication keys to forwarding nodes encrypted with secret keys that will be used for endorsing. The forwarding nodes store the keys if they can decrypt them successfully. Each forwarding node validates the authenticity of the reports and drop the false ones. Later,cluster heads send authentication keys to validate the reports. The DEF[4] scheme involves the usage of authentication keys and secret keys to disseminate the authentication keys; hence, it uses many keys and is complicated for resource-limited sensors.

2.5 Becan

In Bandwidth efficient Cooperative Authentication (BECAN)[5] scheme, each node requires _xed (k)number of neighbors for co-operative neighbor router(CNR) based authentication. BECAN filter in-jected false data through cooperative authentication of the event report by k neighboring nodes of the source node.

BECAN distributes the authentication of en-routing to all sensor nodes along the routing path to avoid complexity. This scheme adopts bit compressed authentication technique to save bandwidth. The proposed technique is suitable to handle compromise and filter injected false data in wireless sensor networks. BECAN is not able to address attacks such as selective dropping and false routing information injected by compromised node.

III. Problem Definition

In the method BECAN (Bandwidth Efficient Cooperative Authentication), if sensor wants to send data to sink, it first finds path and then exchanges key with neighbor. If node is not adversary then only it can send data to neighbor. Finally MAC scheme is used for authentication. Here, injected false data identified earlier as possible. Over head of sink is reduced and energy consumption also very low compared to other methods. BECAN scheme only verifies the packets by using MAC and the keys generated by each node. Sharing pair-wise key with other sensor nodes may be vulnerable as an intermediate node can be compromised and hence keys will be disclosed. As a result, those compromised forwarding nodes can be easily manipulated to inject false data reports by the inside attacker. So security is less in the method.

IV. Prposed System

In order to increase the security of BECAN, can use a different Hybrid Authentication Scheme(HAS) based on RSA with CRT encryption instead of the verification of MAC. As the report is forwarded, each node along the way verifies the correctness of the RSAs probabilistically and drops those with invalid RSAs. As the infield compromised node is prevented from gathering enough RSAs, the report generated by it can be detected and dropped en-route and exclude the attacker node from the network so that injection of false data will be avoided in future. HAS prevents unauthorized access through injecting false data attack from mobile compromised sensor nodes through routing protocols.

V. Implementation Details

The simulation is in NS2 on Linux machine to authenticate the filtering of injected false data in Wireless sensor network. Mainly focus on the link stability and route lifetime, no route overhead was considered in the simulation. In 2500X1000 square meter area, nodes exist. Uses square area to increase average hop length of a route with relatively small nodes. The transmission range is fixed at 250 units. The number of nodes is set as 100. Nodes are assigned with unique ID and keys are generated for each node before deployment. The project includes the following modules:

- Architecture Model
- Power Management
- Key Management
- Security Analysis

VI. Experimental Results

BECAN method with HAS is implemented and the simulated output is obtained. Based on the values from the trace file, graphs are plotted. Compared with the existing method, the energy consumption is low and the throughput is high in this method

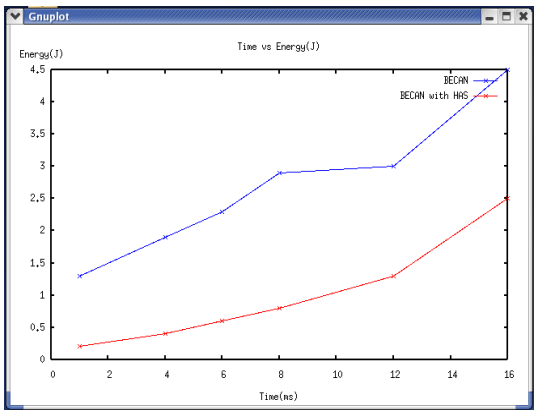

Figure 1: Energy Vs Time graph

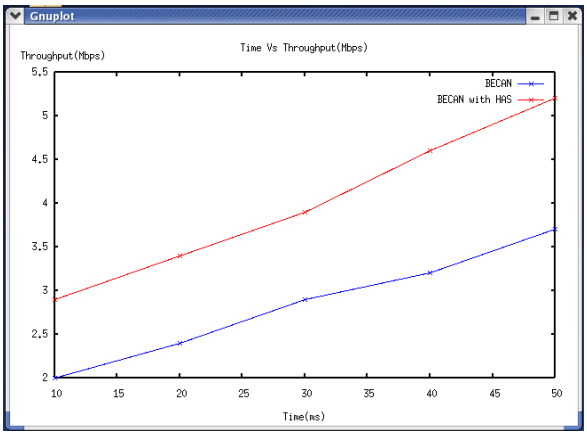

Figure 2: Throughput Vs Time graph

VII. Conclusion

Analyzed about false data injection by compromised node in WSN. En-route Filtering is an efficient way of dealing with false data injection attacks. A literature survey is done to analyzes about the en-route filtering schemes such as SEF, CCEF, STEF, DEF and BECAN. Implemented the BECAN with HAS and analyzed by comparing with existing methods. It shows BECAN with HAS model is efficient than older methods in case of energy consumption and throughput.

References

[1] F. Ye, H. Luo, S. Lu, and L. Zhang. Statistical en-route filtering of injected false data in sensor networks. In INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, volume 4, pages 2446-2457. IEEE, 2004

[2] H. Yang and S. Lu. Commutative cipher based en-route filtering in wireless sensor networks. In Vehicular Technology Conference, 2004. VTC2004 Fall. 2004 IEEE 60th, volume 2, pages 1223-1227.IEEE, 2004.

[3] C. Kraub, M. Schneider, K. Bayarou, and C. Eckert. Stef: A secure ticket-based en-route filtering scheme for wireless sensor networks. In Availability, Reliability and Security, 2007. ARES 2007.The Second International Conference, pages 310-317. IEEE, 2007.

[4] Z. Yu and Y. Guan. A dynamic en-route filtering scheme for data reporting in wireless sensor networks. IEEE/ACM Transactions on Networking(ToN), 18(1):150-163, 2010.

[5] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen. Becan: A bandwidth efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. Parallel and Distributed Systems, IEEE Transacztions , 23(1):32-43,2012.