An Evaluation Of En-Route Filtering Methods For False Data Injection Attack In WSNs

Syama M
M. Tech student,

Deepti C
Asst. Professor

Abstract

Wireless Sensor Networks (WSNs) are vulnerable to various security attacks due to their deployment in hostile environments. These networks are prone to be attacked by adversaries who intend to destruct the proper functioning of network by compromising some of the nodes and inserting false data into the network. The injected false data reports lead the en-route nodes and the sink node to make false decisions. This depletes the energy of nodes and poses a threat to the lifetime of the whole network. This paper reviews some of the existing en-route filtering mechanisms for false data injection attack and evaluates the performance of these methods based on their features and efficiency.

1. Introduction

A WSN consists of numerous autonomous sensors to monitor physical or environmental events comprising of base stations (sinks) and sensing nodes (motes). Each sensor node can sense data such as temperature, humidity, pressure etc from its surroundings .Each node is also capable of conducting simple computations on the collected data .The node can then forward it to other neighboring nodes through wireless communication links. WSNs have drawbacks with regard to limited resources like energy [1], memory [2] and computational power [3]. Hence sensors are designed with light-weight protocols and algorithms, simple architecture, less capacity and centralized data processing for extending network life time.

Sensors are used to detect events in unattended or hostile environment, so security and privacy [4] of sensor nodes is an immense problem of concern. An adversary can capture and compromise some sensor nodes and launch internal attacks. In the false data injection attack [5], an adversary injects false data into the system with the goal of overloading the sink which leads to the depletion of energy resources of the whole network. Due to this, wrong control messages may also be generated En-route filtering, which involves dropping of false data in the routing nodes is an efficient mechanism for avoiding false data. Many en-route filtering schemes exist which are useful for different network models and different applications. The efficiency differs for various schemes. Statistical en-route filtering(SEF), dynamic en-route filtering(DEF), virtual energy-based encryption and keying (VEBEK) and bandwidth efficient cooperative authentication scheme (BECAN) are some of the en-route filtering methods discussed in this paper.

2. Attacks in wsn

Various types of Attacks in WSNs pose potential threats for the efficient functioning of the network.

- A malicious node which is not part of that network masquerades as an external attacker that wants to harm the network.
- An internal attacker who is part of the network and is authorized to access the resources but uses them in an illegitimate way.
- Remote attacks propagate by emitting a high-energy signal to destruct the communication.
- A passive attacker will just drop or monitor packets in a WSN. By modifying routing information and replicating data packets the attackers can cause communication failure.

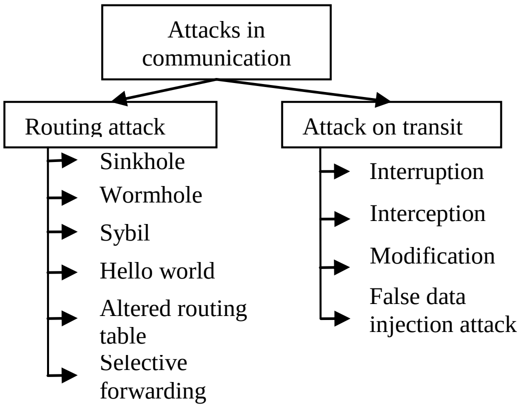

Fig 1. Attacks in WSN

Figure 1 shows the categorization of attacks that affect communication. In routing attack [6] adversaries can gain access to routing path information and redirect the path. These may mislead routing paths, acting as black holes that swallow packets and lead to selective forwarding of packets through selected sensors. Attacks on information transit [7] can be broadly divided as interruption, interception, modification and false data injection attack.

3. False data injection attack

In false data injection attack, an adversary compromises certain nodes and injects false data into the network. False sensing reports also can be injected through the compromised nodes. An adversary can compromise few sensor nodes and gain access to all key elements and take control over that node. The attacker can alter the node or insert false data into the network which can lead to denial of service attack (DOS), black hole attack etc on the network. The compromised nodes can also easily insert false data reports of nonexistent events. The received false data may even cause upper level error decision at the sink. False data reports produce false alarms and also waste valuable network resources, such as energy and bandwidth. Hence it is very important to design an efficient mechanism to prevent and minimize the effect of false data injection attack in WSNs. En-route filtering is one of the effective defense mechanisms against false data injection attack.

3.1. En-Route Filtering

The objective of en-route filtering is to enhance the effectiveness of filtering and improve prevention against node compromise. In en-route filtering both the destination node and intermediate nodes check for the authenticity of the packet and false data is identified as early as possible. Hence the number of hops the false data will travel is reduced and energy is conserved. In the first phase of en-route filtering mechanism, every intermediate node verifies the MAC computed by the previous node in the routing path and then removes that MAC from the received packet. If the verification test is passed, it computes a new MAC based on its pairwise key shared with the next node to which it should forward the packet .This new MAC attaches to the packet. Finally, it forwards the report to the next node in the route.

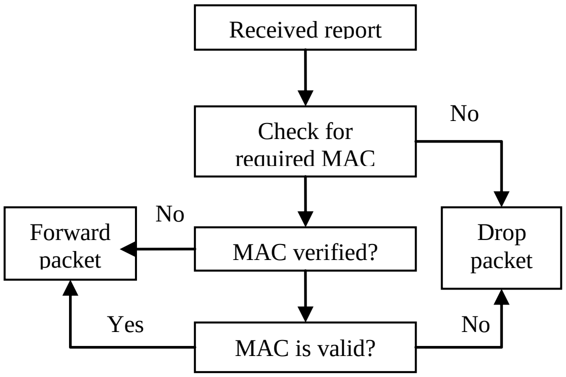

Fig 2. Flow of en-route filtering process

Figure 2 shows the framework of an en-route filtering mechanism. Here the en-route node receives the packet from source node or previous en-route node in the routing path. Then it checks the authenticity of the received packet by verifying the MAC attached in it. If verification of MAC is confirmed then the packet is forwarded to next en-route node in the path or else the packet is dropped.

4. Related works and solutions

Various schemes have been proposed in recent years in the field of sensor network security. These schemes elaborate on the various attacks on sensor network routing protocols and possible ways of defense against it. Internal attack by an adversary cannot be solved by using cryptographic techniques [8]. En-route filtering mechanisms are suitable for defense against such attacks. The false data will be dropped out as early as possible in en-route filtering mechanisms and hence it is also very useful for protection against false data injection attack and DOS attack. DoS attacks have been evaluated in different sensor protocol stack layers [9] and it has been concluded that the security issue should considered at the design phase itself. Sasha[10] et al. proposes the trade-off between overhead and strength of security based on the importance of information. The ways to reduce energy utilization in cryptographic algorithms by using dynamic voltage scaling method is studied by Lin [11]. Carman et al. [12] compares the energy utilization of different asymmetric key algorithms on various types of sensors. Various efficient en-route filtering mechanisms to avoid false data injection attack have been briefly explained below.

4.1 Statistical En-route Filtering (SEF)

SEF [13] consists of a global key pool, which is divided into 'n' nonoverlapping groups. Before deployment of the nodes, a few keys are randomly chosen from one of the group in global key pool and stored in each node. Nodes which have keys from same group in global key pool are considered as the same nodal group. Similarly, all nodes are divided into 'n' nodal groups via non-overlapping key groups. The SEF method performs T-authentication, i.e, the legitimate packet should carry T MACs created by T nodes from different groups. All these T nodes create MAC with any one of the authentication keys stored. Each sensor which detects an event approves the message by generating a keyed MAC by using one of its stored keys. If a message has insufficient number of MACs then it will be dropped. When the message is received at a sink node, the node verifies all the MACs carried in the report since it has the knowledge about whole global key pool. False data with incorrect MACs that may pass the en-route filtering will be definitely detected at the sink. Simulation results and analysis shows that SEF can efficiently detect false data even when the attacker has compromised a number of nodes and has obtained the security keys, if those keys belongs to a small number of key pool groups. SEF can filter out 80 to 90% false data within 10 forwarding hops.

4.2. Dynamic En-Route Filtering (DEF) Scheme

In the Dynamic En-route Filtering (DEF)scheme[14] a legitimate packet is approved by multiple nodes using their own authentication keys. Each node is preloaded with a seed authentication key and secret keys that are randomly chosen from a global key pool, before deployment. Before sending the packet, the cluster head broadcasts authentication keys to en-route nodes encrypted with secret keys that will be used for approval. The en-route nodes store the keys if they can decrypt them successfully. Each en-route node validates the integrity of the packet and drops the false ones. Consequently cluster heads send authentication keys to validate the packet. DEF method involves the usage of authentication keys and secret keys to spread the authentication keys, so it is complicated for resource-limited sensors.

4.3. VEBEK: Virtual Energy-Based Encryption and Keying

VEBEK [15] is a secure network protocol for wireless sensor Network (WSN). It uses one-time dynamic key for one packet generated by the source node, so it reduces the overhead of refreshing keys. RC4[] encryption mechanism is used here to provide confidentiality of the data. The key for encryption is generated from Virtual Energy based keying module. To decode and authenticate a message the receiving node must keep track of the energy of the sending node. When an en-route node receives the packet, it verifies its watch list to confirm that the packet came from a node it is watching. If verification fails, the packet is forwarded without modification.

VEBEK provides two operational modes VEBEK-I and VEBEK-II. In VEBEK-1 mode all nodes watch their neighbors and when a packet is received from a neighboring node, its authenticity and integrity are verified. It can catch the malicious node in one hop itself and hence transmission overhead is minimized. But processing overhead is increased due to the decode/encode that occurs at each hop. In VEBEK-II mode, node in the network is organized to watch some of the nodes and it cannot find malicious packets in one hop. More energy will be spent for node synchronization and this leads to overhead for the node.

4.4. A Bandwidth-Efficient Cooperative Authentication (BECAN) Scheme

BECAN [16] shows high filtering and reliability compared to other en-route filtering methods. In this method, co-operative neighbor router (CNR) based authentication is used and hence each node requires a fixed number of neighbors. BECAN filters inject false data through cooperative authentication of the event report by fixed 'k' neighboring nodes of the source node. BECAN distributes the authentication of en-route to all sensor nodes in the routing path to minimize complexity. It uses bit compressed authentication technique to reduce bandwidth utilization. Selective dropping, false routing information from compromised node etc cannot be handled by using BECAN.

5. Performance analysis of en-route filtering schemes

Performance of the en-route filtering mechanisms are evaluated based on false data filtering hops and energy consumption in terms of amount of authentication messages transferred. SEFs filtering capacity is limited and cannot address impersonating attacks. Here single shared key is used for creating and verifying MACs. Hence misuse of keys may occur to generate packets. DEF has higher filtering capacity. DEF and SEF are independent of topology changes. It can filter only those unauthorized nodes with no session key. It cannot identify the false data injected from compromised cluster-head or any other sensor nodes. DEF filtering techniques are more attack resilient than static techniques. A significant drawback is that the communication overhead is increased due to refreshing of keys or redistribution from time to time in the network. The reasons for key refreshing includes updating keys after revocation, to avoid key from becoming old, or due to dynamic changes in the topology of network. DEF is more complicated than SEF because of extra control messages and it leads to operation complexity and extra overheads. DEF is complicated mainly for resource limited sensors. BECAN is energy efficient with reduced bandwidth utilization. BECAN can filter false data injection attack but it cannot detect other attacks caused by compromised nodes.

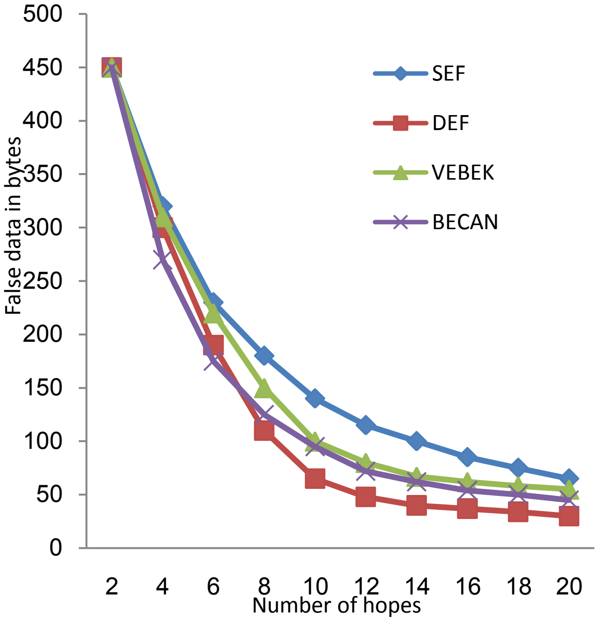

Fig 3. The graph showing the filtering rate for SEF, DEF, VEBEK and BECAN

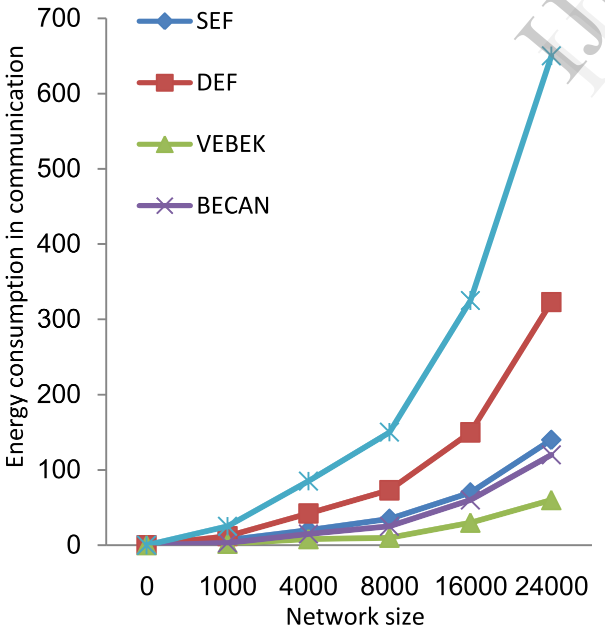

Fig 4. The graph showing the energy efficiency for SEF, DEF, VEBEK and BECAN

Figure 3 explains the filtering rate for SEF, DEF, VEBEK and BECAN with respect to number of hops of data transmission. Figure 4 shows the energy efficiency of each by considering the size of network. Total energy consumption is directly proportional to the number of transmissions that is the sum of the number of data packets and control packets sent per node.

Table 1 describes the performance of various en-route filtering mechanisms. The efficiency of the en-route filtering mechanisms can be evaluated based on the amount of messages used to authenticate the event packet, filtering capability of each en-route node on the data transfer path and amount of energy utilized for filtering the false data. Performance evaluation shows that VEBEK consumes less energy compared to other techniques. DEF filters the false data as fast as possible but an additional amount of authentication messages are required as compared to other methods.

Table 1: Performance analysis of different en-route filtering methods

Filtering method	Authentication message	False data filtering with hops	Energy efficiency
Statistical En-Route Filtering	Event report contains MAC from all detecting nodes.	90% of false data is dropped within 20 hops	80% of energy saved
Dynamic En-Route Filtering	Event report contain authentication message from all nodes in the cluster	90% of false data is dropped within 10 hops	50% of energy saved
VEBEK	Event report contains energy value of a sending node and node id.	90% of false data is dropped within 15 hops	60-100% of energy saved
BECAN	Each report contain authentication message from all neighboring nodes each represented in one bit	90% of false data is dropped within 15 hops	80% of energy saved

Table 2 describes the features and drawbacks of various en-route filtering mechanisms. It shows that each filtering method is efficient for different network models and applications. The filtering technique should be chosen according to the situation and requirements.

6. Conclusion

This paper discusses the security issues of WSN in particularly false data injection attack. False data injection attack is dangerous since it results in false decision making and high energy wastage in the network. It is clear that en-route filtering mechanism is an effective method for defending false data injection attack. A review of different en-route filtering mechanisms such as statistical en-route filtering, dynamic en-route filtering, VEBEK and BECAN are discussed here. The performance evaluation of these filtering methods has been done by analyzing number of authentication messages transferred with the actual data. The analysis shows that different filtering methods are useful for different network models and applications.

Table 2: Analysis of various en-route filtering methods

Filtering method	Uses	Network model	Features	Drawbacks
Statistical En-Route Filtering	False data injection attack, Information spoofing	Highly dense WSNs	1. Detects and drops false report Multiple detecting nodes jointly produce event report	1. Inefficient if the number of compromised node exceeds a threshold value
Dynamic En-Route Filtering	False data injection attack, Selective forwarding	Sensor nodes are organized into clusters	1. For key dissemination Hill Climbing approach is used. 2. Earlier false data filtering. 3. Each node requires key chain for authentication.	1. More complicated because of extra control messages. 2. Extra control messages causes tripling of delay of reports.
VEBEK	False data injection attack, Eavesdrops of packets	Randomly distributed sensor nodes	1. Key based on residual energy 2. Improves synchronization problem	1. Extra energy is needed for synchronization 2. Fixed path for data delivery.
BECAN	False data injection attack	Randomly distributed sensor nodes	1. Bit-compressed authentication 2. Cooperative neighborhood based filtering mechanism 3. High reliability	1. Cannot detect false data injected by compromised node. 2. Cannot filter gang false data injection attack.

References

[1] F.Akyildiz Su, Y. Sankarasubramaniam, ”A survey on sensor Networks” ,IEEE communication magazine vol.40,no.8,pp.102-114,Aug 2002.

[2] Yang xiao, Venkata Krishna Rayi, Bo Sun,Xiao jiang Du,”A Survey of key management schemes in wireless sensor networks ”Elsevier publication vol 30,pp2314-2341,2007.

[3] Yun Zhou,Y.fany,”securing wireless sensor networks a survey”IEEE communication survey & Tutorials vol. 10,no.3,2008.

[4] H. Chan and A. Perrig, “Security and privacy in sensor networks,” *IEEE Computer Magazine*, pp. 103–105, 2003.

[5] Mo, Yilin Garone, Emanuele; Casavola, Alessandro; Sinopoli, Bruno, "False data injection attacks against state estimation in wireless sensor networks",Decision and Control (CDC), 2010 49th IEEE Conference on Date of Conference: 15-17 Dec. 2010.

[6] C. Hartung, J. Balasalle, and R. Han, “Node compromise in sensor networks: The need for secure systems”, Technical Report CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.

[7] J. A. Al-Karaki and A. E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” IEEE Wireless Commun., vol.11, no. 6, Dec. 2004.

[8] Kai Xing, Shyaam Sundhar Rajamadam Srinivasan, Manny Rivera, Jiang Li, Xiuzhen Cheng "Attacks and Countermeasures in Sensor Networks: A Survey"2005 Springer

[9] A.D. Wood and J.A. Stankovic, “Denial of service in sensor networks”, IEEE Computer, Vol. 35, No. 10, pp. 54-62, 2002.

[10] D. Djenouri, L. Khelladi, A. N. Badache, "A survey o f security issues in mobile ad hoc and sensor networks", IEEE Communications Surveys & Tutorials 7 (4) (2005) 2–28.

[11] S. Slijepsevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. Srivastava, "On Communication Security in Wireless Ad-Hoc Sensor Networks," in *11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2002.

[12] L. Yuan and G. Qu, "Design Space Exploration for Energy-Efficient Secure Sensor Networks," in *IEEE International Conference on Application-Specific Systems, Architectures and Processors*, 2002.

[13] D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and Approaches for Distributed Sensor Network Security," NAI Labs, Tech. Rep. 00-010, September 2000.

[14] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Detection and Filtering of Injected False Data in Sensor networks," Proc. IEEE INFOCOM "04, Mar. 2004.

[15] H. Hou, C. Corbett, Y. Li, and R. Beyah, "Dynamic Energy-Based Encoding and Filtering in Sensor Networks," Proc. IEEE MilitaryComm. Conf. (MILCOM '07), Oct. 2007.

[16] Arif Selcuk Uluagac, Yingshu Li, "VEBEK: Virtual Energy Based Encryption and keying for wireless sensor networks"IEEE Transaction on mobile computing vol. 9, No.7, July 2010.

[17] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, and Xuemin (Sherman) Shen, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 1, January 2012.

Authors

Ms Syama M received her Bachelor of Engineering in Computer Science and Engineering from CUSAT University in 2011. She is pursuing her M. Tech in Computer Networking from Visvesyaraya Technological University. Her area of interest is security in wireless networks.

Mrs. Deepti C received her Bachelor of Engineering in Electronics and Communication in 2004. She received her M.Tech in Computer Network Engineering with distinction from Visvesvaraya Technological University in 2009.She is a PhD student in Electronics and Communication Engineering at Christ University, Bangalore. Currently she also holds a faculty position as Assistant Professor, Department of ISE, The Oxford College of Engineering. Her main research interests are signal processing, wireless sensor networks and wireless network security.