Threshold Determination Method For Dynamic En-Route Filtering In WSN

Pandimurugan[1], J Mary Suji Mol[2], Abraham[3]
[1,2,3]Assistant Professor
[1, 3]Hindustan Institute of Technology and Science
[2]Jeppiaar SRR Engg College

Abstract- *In wireless sensing element network include an outsized range of tiny sensing element nodes, this sensing element nodes organized into cluster and send some report back to base station. This sensing element networks could suffer differing kinds of malicious attacks. One kind is termed wrong report injective attack, during which adversaries push into sensing element networks the false knowledge reports containing nonexistent events or faked readings from compromised nodes. These attacks not solely cause false alarms at the bottom station, however additionally drain out the restricted energy of forwarding nodes. Also, the adversaries could launch DoS attacks against acceptable reports. In selective forwarding attacks, they will by selection drop legitimate reports, whereas in report disruption attacks they will designedly contaminate the authentication info of legitimate reports to create them filtered out by alternative nodes. There square measure several offered theme for filtering the false knowledge injection, they're SEF, IHA, CCEF and semiconductor diode are projected to deal with wrong report injective attacks and/or DoS attacks. we tend to propose Dynamic en-route filtering theme that address each false knowledge injection and Dos attacks in wireless sensing element networks. In our theme, sensing element nodes square measure organized into clusters. every acceptable report ought to be valid by multiple message authentication codes (MACs), that square measure made by sensing nodes victimisation their own authentication keys. The authentication keys of every node square measure created from a hash chain. Before causing reports, nodes air their keys to forwarding nodes victimisation Hill rise approach. Then, they send reports in rounds.*

Keywords- wireless sensors, security attack, network security, dynamic filtering.

I. INTRODUCTION

In wireless sensor network consist of a large number of small sensor nodes, this sensor nodes organized into cluster and send some report to base station. This sensor networks may suffer different types of malicious attacks. One type is called false report injection attack, in which adversaries inject into sensor networks the false data reports containing non-existent 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(1). In selective forwarding attacks, they will significantly drop acceptable reports, whereas in report tumultuous attacks they will designedly contaminate the authentication info of acceptable reports to create them filtered out by alternative nodes. We propose Dynamic en-route filtering scheme that address both false data injection and Dos attacks in wireless sensor networks.

There are many existing theme for filtering the false knowledge injection, they're SEF, IHA, CCEF and semiconductor diode are projected to deal with false report injection attacks and/or DoS attacks. and that they have some limitation..

- SEF is independent of network topology, but it has limited filtering capacity and cannot prevent impersonating attacks on legitimate nodes.
- IHA has a drawback, that is, it must periodically establish multihop pairwise keys between nodes. 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 (2).
- CCEF also relies on the fixed paths as IHA does and it is even built on top of high cost public-key operations. More severely, it does not support en-route filtering.
- LEDS utilize location-based keys to filter false reports. They 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.

II. DYNAMIC EN-ROUTE FILTERING SCHEME

A dynamic en-route filtering theme to deal with each false report injection attacks and DoS attacks in wireless sensing element networks. In our theme, sensing element

nodes square measure organized into clusters. every acceptable report ought to be valid by multiple message authentication codes (MACs), that square measure made by sensing nodes victimisation their own authentication keys. The authentication keys of every node square measure created from a hash chain (3). Before causing reports, nodes air their keys to forwarding nodes victimisation Hill rise approach. Then, they send reports in rounds. In every round; each sensing node endorses its reports employing a original key and so disposes the key to forwarding nodes. victimisation the disseminated and disclosed keys, the forwarding nodes will validate the reports. In our theme, every node will monitor its neighbours by overhearing their broadcast, that prevents the compromised nodes from dynamic the reports (5). Report forwarding and key revealing square measure repeatedly dead by every forwarding node at each hop, till the reports square measure born or delivered to the bottom station.

III. ARCHITECTURE OF DYNAMIC EN-ROUTE FILTERING

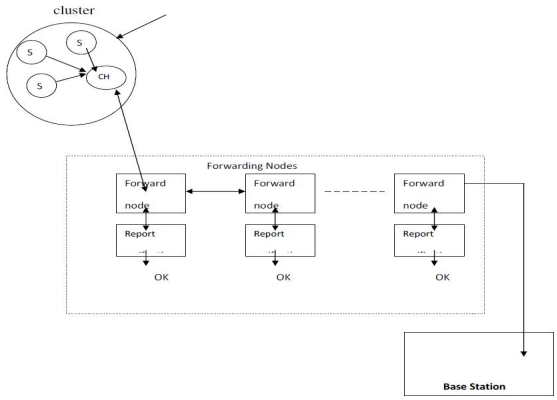

Figure 1: Architecture Of Dynamic En-Route Filtering

A dynamic en-route filtering scheme used to drop the false report in wireless sensor network. In the network each sensing nodes uses its own auth-keys to authenticate their reports. 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 each 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(4). Our Hill Climbing key dissemination approach increases filtering capacity greatly and balances the memory requirement among nodes. Each node has multiple downstream nodes that possess the necessary key information and are capable of filtering false reports. This not only makes our scheme adaptive to derivatively dynamic networks, but also mitigates the important of selective forwarding attacks. Monitored by its upstream nodes and neighbors, the compromised nodes have no way to contaminate legitimate reports or generate false control messages.

IV. KEYS PHASES OF EN-ROUTE FILTERING

In the key pre-distribution phase each sensor nodes preloaded with distinct seed key. From the seed key, it can generate a sequence of auth-keys using a common hash function. Using these auth-keys to encrypt the report and forward at the base station. The first key of the hash chain, also it should be used first at the encryption process; meanwhile (8), it is the final one generated from seed key. We assume that the base station is aware of each node's seed key, so the adversaries cannot impersonate the uncompromised nodes. the primary key of the hash chain, additionally it ought to be used 1st at the coding process; meantime, it's the ultimate one generated from the seed key. we tend to assume that the bottom station is responsive to every nodes seed key, that the adversaries cannot impersonate the uncompromised nodes. The key per-distribution part is performed before the sensing element nodes square measure deployed. within the key dissemination part the sensing nodes organized because the cluster, type that cluster head haphazardly elect. This part can happen before causing the report. During this part the cluster head aggregates the auth-keys of the sensing nodes and also the cluster-head ought to air the primary auth-keys of all nodes to the forwarding nodes before causing the reports (10). By victimisation the disseminated keys, the forwarding nodes will verify the credibility of the disclosed auth-keys, that square measure successively wont to check the validity and integrity of the reports. the primary unused auth-key of a node is termed the present auth-key of that node. once none of a nodes auth-keys has ever been used, the present auth-key is simply the primary auth-key of its hash chain. Report forwarding phases the sensing nodes forwarding the report back to base station. The reports square measure organized into rounds, every containing a hard and fast range of reports. In each spherical, every sensing node chooses a brand new auth-key to manifest its reports. To facilitate verification of the forwarding nodes, the sensing nodes disclose their auth-keys at the tip of every spherical. Meanwhile, to forestall the forwarding nodes from abusing the disclosed keys, a forwarding node will receive the disclosed auth-keys, solely once its upstream node overhears that it's already broadcast the reports. Receiving the disclosed keys, every forwarding node verifies the reports, and informs its next-hop node to forward or drop the reports supported the verification result (9). If the reports square measure valid, it discloses the keys to its next-hop node once overhearing. The processes of verification, overhearing, and key revealing square measure recurrent by the forwarding nodes at each hop

till the reports square measure born or delivered to the bottom station.

V. SENSOR CLUSTERING NODES

A acceptable packet is approved by multiple nodes using their own authentication keys in the Dynamic En-route Filtering (DEF) scheme . Before deployment each node is preloaded with a seed authentication key and secret keys that are randomly chosen from a global key pool. The cluster head broadcasts authentication keys to en-route nodes encrypted with secret keys before sending the packet, that will be used for approval. If they can decrypt them successfully then enroute nodes store the keys (11). 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. To spread the authentication keys, DEF method involves the usage of authentication keys and secret keys.

1. All the nodes in the network are initialized w.r.to to a master key 'M', Master key is used to launch the key divided in between neighboring nodes in the every cluster. Each node has been designate by a unique ID and each nodes stores IDs of that neighbors to form cluster.
2. The node ID is stored in the node before it distributed. A network designer assign the cluster ID to each and every cluster and each sensing node hold its cluster ID, e.g., each and every sensing node in cluster CHi keep the cluster IDCi in its memory.
3. After assigning IDs the nodes in the network are initiated. {M, Mc, f(x,y,z),T, H(.)}. Where, - Mc is the set of master keys (central) in the clusters of nodes, - f(x,y,z) Primitive polynomial of cluster Ci with parameter x; y and z. - T is threshold set of polynomials. - H is the hash function. 2. Authentication polynomial of node S1 auth (S1) = α f(S1, y, z), 3. Check polynomial of node S1 Verf (S1) = β f(S1, x, z). 4. Reports r1, r2, ……. , rn. are generated by Report r = ((E)KCHi. — x — MAP)
4. 5. MAP is Message authentication polynomial which is generated by each sensing nodes by, MAP = authr(y, z) = α f(S1, y, H((E) Kc,)) Where, - E = measured invigilator element, - H(·) is the hash function hold in node Si = KCi is the cluster key, to which Si belongs, and the node Si creates MAP for the measurement
5. Report along with MAP are sent to forwarding node.
6. Forwarding node performs polynomial based filtering and forwards report only if following conditions are satisfied. Condition 1: The time stamp t connected to the report should be refreshing. Condition 2: T MAPs connected in the result or report should be different and created by the sensing nodes. Condition 3: T MAPs can be checked by the intermediate node using stored check polynomial.
7. Controller performs filtering same as forwarding node.
8. If report is valid, it decrypts and sends to respected cluster head.

VI. CONCLUSION

In this paper, we propose 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 eports. This process is repeated by each forwarding node at every hop.

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] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proc. ACM CCS, 2003, pp. 52–56.
[10] D. Nicolescu and B. Nath, "Ad-hoc positioning systems (APS)," in Proc. IEEE GLOBECOM, 2001, vol. 5, pp. 2926–2931.
[11] 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] 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. IEEE INFOCOM, 2006, pp. 1–12