Adversary Detection in Wireless Sensor Networks Under Byzantine Attacks

P. Sathya Priya, S. Lokesh

Abstract— **This work discovers reliable data fusion which overcome coverage problem in mobile access wireless sensor networks under Byzantine attacks. Consider the q-out-of-m rule, in which final decision is made based on the q sensing reports out of m polled nodes and can achieve a good trade-off between the miss detection probability and the false alarm rate. In this work, first, propose a simplified, topology construction which construct and maintains an efficient network topology. Second, propose a multicast message transmission where multicasting requires special techniques that make clear who is in the intended group of recipients. Finally, propose a simple and effective malicious node detection approach, where the malicious sensors are identified by comparing the decisions of the individual sensors with that of the fusion center. This work further proposes the adversary node detection approach and adapts the fusion parameters based on the detected malicious sensors. Simulation examples are presented to illustrate the performance of proposed approaches.**

Index Terms— **Sensor networks, Byzantine attacks, q-out-of-m rule.**

I. Introduction

Wireless sensor networks (WSNs) have been studied intensively for various applications such as environment monitoring, area monitoring and landslide detection [1]. They usually consist of a processing unit with limited computational power and limited memory, sensors, a communication device, and a power source usually in the form of battery [3]. A serious threat to wireless sensor networks is the Byzantine attack [5], where the adversary has full control over some of the authenticated nodes and can perform arbitrary behavior to disrupt the system. Byzantine fault encompasses both omission failures as failing to receive a request, or failing to send a response and commission failures as processing a request incorrectly. The MA receives the sensing reports and applies the fusion rule to make the final decision. One popular hard fusion rule used in distributed detection is the q-out-of-m scheme [4], in which the mobile access point randomly polls reports from m sensors, then decides that the target is present only if q or more out of the m polled sensors report ‘1’. It is simple to implement, and can achieve a good tradeoff between minimizing the miss detection probability and the false alarm rate. In ideal scenarios, the optimal scheme parameters for the q-out-of-m fusion scheme are obtained through exhaustive search. However, due to its high computational complexity, the optimal q-out-of-m scheme is infeasible as the network size increases and/or the attack behavior changes. To overcome this limitation, effective sub-optimal schemes with low computational complexity are highly desired.

First, propose a simplified, topology construction which construct and maintains an efficient network topology. Once the initial topology is deployed, especially when the location of the nodes is random, the administrator has no control over the design of the network; for example, some areas may be very dense, showing a high number of redundant nodes, which will increase the number of message collisions and will provide several copies of the same information from similarly located nodes. However, the administrator has control over some parameters of the network, transmission power of the nodes, state of the nodes, role of the nodes, etc. by modifying this parameters, the topology of the network can change.

Second, propose a multicast message transmission where multicasting requires special techniques that make clear who is in the intended group of recipients. Messages are sent to a group of stations that meet a particular set of criteria.

Finally, propose a simple and effective adversary node detection approach, where the malicious sensors and adversary sensors are identified by comparing the decisions of the individual sensors with that of the fusion center. It is observed that dynamic attacks generally take longer time and more complex procedures to be detected as compared to static attacks. It is also found that the proposed adversary detection procedure can identify adversarial sensors accurately if sufficient observation time is allowed. It is shown that the proposed adaptive fusion scheme can improve the system performance significantly under both static and dynamic attack strategies.

II. LITERATURE SURVEY

A. *Distributed Deployment Scheme*

In wireless sensor networks (WSNs) multi-level (k) coverage of the area of interest can be achieved by solving the k-coverage sensor deployment problem. A WSN usually consists of numerous wireless devices deployed in a region of interest, each able to collect and process environmental information and communicate with neighboring devices. Sensor deployment is an essential issue in WSN because it not only determines the cost to construct the network but also affects how well a region is monitored by sensors. In particular, given a region of interest, we say that the region is k-covered if every location in that region can be monitored by at least k sensors, where k is a given parameter. A large amount of applications may impose the requirement of k > 1. For instance, military or surveillance applications with a stronger monitoring requirement may impose that k > 2 to avoid leaving uncovered holes when some sensors are broken. Consider two sub-problems: k-coverage sensor placement problem and distributed sensor dispatch problem. The

Manuscript received December 10, 2013.

P. Sathya Priya, Computer Science and Engineering, Hindusthan Institute of Technology, Pollachi, India. 9659499974.

S. Lokesh, Computer Science and Engineering, Hindusthan Institute of Technology, Pollachi, India. 9865723232.

placement problem asks how to decide the minimum number of sensors required and their locations in I to ensure that I is k-covered and that the network is connected. Note that coverage is affected by sensors' sensing distance, while connectivity is determined by their communication distance.

Considering that sensors are mobile and the area I may change over time, the objective of the dispatch problem is to schedule sensors to move to the designated locations (according to the result computed by the placement strategy) such that the total energy consumption of sensors due to movement can be minimized. For coverage, consider both the binary and probabilistic sensing models of sensors. Under the binary sensing model, a location can be monitored by a sensor if it is within the sensor's sensing region.

$$p(u, s_i) = \begin{cases} e^{-\varepsilon d(u, s_i)}, & \text{if } d(u, s_i) \le r_s, \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

where ε is a parameter indicating the physical characteristics of the sensor and d(u, s_i) is the distance between u and s_i. In this way, a location in A is considered as k-covered if the probability that there are at least k sensors which can detect this location is no smaller than a predefined threshold p_{th}, where 0 < p_{th} < 1. With the above definitions, an area in A is considered as k- covered if every location inside that area is k-covered.

B. Cut Detection

A wireless sensor network can get separated into multiple connected components due to the failure of some of its nodes, which is called a "cut". Failure of a set of nodes will reduce the number of multihop paths in the network. Such failures can cause a subset of nodes that have not failed to become disconnected from the rest, resulting in a "cut." Two nodes are said to be disconnected if there is no path between them. assume that there is a specially designated node in the network, which we call the source node. The source node may be a base station that serves as an interface between the network and its users. Since a cut may or may not separate a node from the source node, which distinguish between two distinct outcomes of a cut for a particular node. When a node u is disconnected from the source, say that a Disconnected from Source (DOS) event has occurred for u. When a cut occurs in the network that does not separate a node u from the source node, say that Connected, but a Cut Occurred Somewhere (CCOS) event has occurred for u. Without the knowledge of the network's disconnected state, it may simply forward the data to the next node in the routing tree, which will do the same to its next node, and so on. However, this message passing merely wastes precious energy of the nodes; the cut prevents the data from reaching the destination. Therefore propose a distributed algorithm to detect cuts, named the Distributed Cut Detection (DCD) algorithm. The algorithm allows each node to detect DOS events and a subset of nodes to detect CCOS events. The DOS detection part of the algorithm is applicable to arbitrary networks; a node only needs to communicate a scalar variable to its neighbors. The CCOS detection part of the algorithm is limited to networks that are deployed in 2D euclidean spaces, and nodes need to know their own positions.

II. MODULES DESIGN

The project contains four main modules.

- Topology Construction
- Multicast Message Transmission
- Find Adversarial Node
- Tree Maintenance.

A. Topology Construction

In this module, construct a topology structure. Here we use mesh topology because of its unstructured nature. Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user. While getting each of the nodes, their associated port and ip address is also obtained. For successive nodes, the node to which it should be connected is also accepted from the user.

While adding nodes, comparison will be done so that there would be no node duplication. Then identify the source and the destinations.

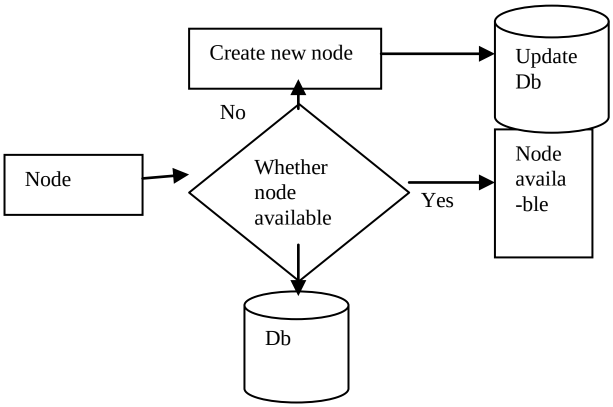

Fig. 1. Topology Construction.

B. Multicast Message Transmission

The requester signs and unicast on the selected route a multicast activation (MACT) message that includes its identifier, the group identifier, and the sequence number used in the RREQ phase. The MACT message also includes a one-way function applied on the tree token extracted from RREP, frequenter; tree token, which will be checked by the tree node that sent the RREP message to verify that the node that activated the route, is the same as the initial requester. An intermediate node on the route checks if the signature on MACT is valid and if MACT contains the same sequence number as the one in the original RREQ. The node then adds to its list of tree neighbors the previous node and the next node on the route as downstream and upstream neighbors, respectively, and sends MACT along the forward route. During the propagation of the MACT message, tree neighbors use their public keys to establish pair wise shared keys, which will be used to securely exchange messages between tree neighbors.

The source periodically signs and sends in the tree an MRATE message that contains its data transmission rate _0. As this message propagates in the multicast tree, nodes may add their perceived transmission rate to it. Each tree node keeps a copy of the last heard MRATE packet. The information in the MRATE message allows nodes to detect if tree ancestors perform selective data forwarding attacks. Depending on whether their perceived rate is within acceptable limits of the rate in the MRATE message, nodes Alternate between two states. The initial state of a node is disconnected; after it joins the multicast group and becomes aware of its expected receiving data rate, the node switches to the connected state. Upon detecting selective data forwarding attack, the node switches back to the disconnected state.

C. Find Adversarial Node

Wireless-specific attacks such as flood rushing and wormhole were recently identified and studied. RAP prevents the rushing attack by waiting for several flood requests and then randomly selecting one to forward, rather than always forwarding only the first one. Techniques to defend against wormhole attacks include Packet Leashes, which restricts the maximum transmission distance by using time or location information, Truelink, which uses MAC-level acknowledgments to infer if a link exists or not between two nodes, and the work in , which relies on directional antennas. Watchdog relies on a node monitoring its neighbors if they forward packets to other destinations. SDT and Ariadne use multipath routing to prevent a malicious if the sender node forward packet to other destinations. If a node does not overhear a neighbor forwarding more than a threshold number of packets, it concludes that the neighbor is adversarial. Use multipath routing to prevent a malicious node from selectively dropping data.

D. Tree Maintenance

We assume a tree-based on-demand multicast protocol, which maintains bidirectional multicast trees connecting multicast sources and receivers. Each tree defines a multicast group. The multicast source is a special node, the group leader, whose role is to eliminate stale routes and coordinate group merges. Route freshness is indicated by a group sequence number updated by the group leader and broadcast periodically as a message in the entire network. For convenience, we call this message a Group Hello message. Higher group sequence numbers denote fresher routes.

Three main operations ensure the tree maintenance: tree pruning, broken-link repair, and tree merging. Tree pruning occurs when a group member that is a leaf in the multicast tree decides to leave the group. To prune itself from the tree, the node sends a message to indicate this to its parent. The pruning message travels up the tree causing leaf nodes that are not members of the multicast group to prune themselves from the tree, until it reaches either a non-leaf node or a group member. A non-leaf group member must continue to act as a router and cannot prune itself from the multicast tree.

III. CONCLUSIONS

In this work, the reliable data fusion is provided for wireless sensor networks under Byzantine attacks where fusion center randomly polls m out of n users and relies on q-out-of-m rule for final decision. The proposed work simplifies construction of initial topology and multicast message transmission among group of nodes. An important observation is that, even if the percentage of adversary sensors remains fixed, the false alarm rate diminishes exponentially with the network size. This implies that for a fixed percentage of adversary nodes, network performance can be significantly improved by increasing the density of the nodes. Furthermore, obtain an upper bound on the percentage of adversary nodes that can be tolerated using the q-out-of-m rule. It is found that the upper bound is determined by the sensors' detection probability and the attack strategies of the malicious and adversary nodes. It is observed that nodes launching dynamic attacks take longer time and more complex procedures to be detected as compared to those conducting static attacks. The adaptive fusion procedure has shown to provide significant improvement in the system performance under both static and dynamic attacks. As to future work, adaptive detection can be conducted under Byzantine attacks and soft decisions can be made based on the sensing reports.

REFERENCES

[1] Y.-C. Wang and Y.-C. Tseng, "Distributed deployment schemes for mobile wireless sensor networks to ensure multilevel coverage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 9, pp. 1280 – 1294, Sept. 2008.

[2] P. Barooah, H. Chenji, R. Stoleru, and T. Kalmar-Nagy, "Cut detection in wireless sensor networks," IEEE *Transactions on Parallel and Distributed Systems*, vol. 23, no. 3, pp. 483 – 490, Mar. 2012.

[3] C. Chong and S. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247– 2056, Aug. 2003.

[4] R. Niu and P. Varshney, "Performance analysis of distributed detection in a random sensor field," *IEEE Transactions on Signal Processing*, vol. 56, no. 1, pp. 339 – 349, Jan. 2008.

[5] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attack ," *IEEE Transactions on Signal Processing*, vol. 57, no. 1, pp. 16 –29, Jan. 2009.

[6] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *Signal Processing, IEEE Transactions on*, vol. 59, no. 2, pp. 774 – 786, Feb. 2011.

[7] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 162–175, 2004.

[8] H. Kumar, D. Sarma, and A. Kar, "Security threats in wireless sensor networks," *IEEE Aerospace and Electronic Systems Magazine*, vol. 23, no. 6, pp. 39 –45, Jun. 2008.

[9] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromise-resilient message authentication in sensor networks," *IEEE 27th Conference on Computer Communications, INFOCOM 2008*, pp. 1418 – 1426, Apr. 2008.

[10] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: Detect malicious nodes in collaborative spectrum sensing," *IEEE Global Telecommunications Conference, GLOBECOM 2009*, pp. 1 –6, 2009.

[11] M. R. Fellows, F. V. Fomin, D. Lokshtanov, F. Rosamond, S. Saurabh, and Y. Villanger, "Local search: Is brute-force avoidable?" *Journal of Computer and System Sciences*, vol. 78, no. 3, pp. 707 – 719, 2012.

[12] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," *Proceedings of the 13th ACM conference on Computer and communications security, ACM CCS 2006*, pp. 278 – 287, 2006.

P. Sathya Priya received the B.E. degree in Computer Science and Engineering from Anna University in 2012 and currently pursuing M.E. degree in Computer Science and Engineering at Anna University. The current research focuses on secure communications in sensor networks.

S. Lokesh received the B.E. and M.E. degrees in Computer Science and Engineering from Anna University in 2003 and 2005, respectively. Currently working as Asst. professor in department of Computer Science and Engineering at Hindusthan Institute of Technology. His major research interests are in network security, wireless networks, and future Internet architectures.