Detection of Malicious Node in EDA Acknowledgement Process

Seyed Amin Ahmadi Olounabadi[1], Avula Damodaram[2], V Kamakshi Prasad[3], PVS Srinivas[4]

[1]Research scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Hyderabad (JNTUH), Hyderabad, Telangana.

[2]Professor, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Hyderabad (JNTUH), Hyderabad, Telangana

[3]Professor & Director of DE, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Hyderabad (JNTUH), Hyderabad, Telangana

[4]Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana

Email: saminahmadi@hotmail.com

Abstract:

Wireless sensor networks are often used to monitor physical and environmental conditions in various regions where human access is limited. Due to limited resources and deployment in hostile environment, they are vulnerable to faults and malicious attacks. The sensor nodes affected or compromised can send erroneous data or misleading reports to base station. Hence identifying malicious and faulty nodes in an accurate and timely manner is important to provide reliable functioning of the networks. In this paper, we present a malicious and malfunctioning node detection scheme using dual-weighted trust evaluation in a hierarchical sensor network. Malicious nodes are effectively detected in the presence of natural faults and noise without sacrificing fault-free nodes. Simulation results show that the proposed scheme outperforms some existing schemes in terms of mis-detection rate and event detection accuracy, while maintaining comparable performance in malicious node detection rate and false alarm rate.

Keywords: *Wireless Sensor Networks; Fault Detection; Malicious Node Detection.*

Introduction:

Wireless sensor networks are often deployed in an unattended area of interest for the purpose of remote monitoring in a homogeneous or heterogeneous environment [1]. Sensor nodes comprising the networks, in practice, have limited power, memory, and computational capabilities. Such networks are vulnerable to faults and malicious attacks. Hence it is important to detect faulty or malicious nodes in the networks to make correct decisions in the monitoring applications.

Several fault detection and tolerance schemes for wireless sensor networks have been proposed in the literature [2-9]. They are developed based on centralized, distributed, and hierarchical models. Due to the importance of energy efficiency, most schemes employ a distributed model, using either neighbor coordination or clustering. These fault detection schemes mainly deal with noise with a certain distribution or randomly and independently generated faults. Malicious nodes, however, have not been deeply investigated, although they are likely to exist in wireless sensor networks due to resource constraints, unreliable communications, and unattended operation.

There are a number of attacks that an attacker can launch against wireless sensor networks once a certain number of sensor nodes have been compromised [10]. In the network and routing layer, the attacks include selective forwarding, sinkholes [11], Sybil [12], wormholes [13], HELLO flood attacks [11], black hole attack [14], and DDOS attacks [15], etc. In application layer, attackers may compromise sensor nodes and inject false data to fool data aggregators. To cope with the attacks both prevention-based and detection schemes have been investigated.

Curiac et al. [16] proposed a malicious node detection scheme using an autoregression technique. It uses time series of measured data provided by each sensor node and relies on autoregressive predictor placed in base stations. Signal strength is used to detect malicious nodes in [17], where a message transmission is considered suspicious if the strength is incompatible with the originator’s geographical position. Several trust management schemes have been proposed primarily in routing and communication. Various efforts have also been made to combine communication and data trusts [18].

A special type of attack where the compromised nodes behave normally but report false readings to lead to an incorrect decision has recently been investigated in [19, 20]. Atakli et al. [19] proposed a novel scheme for detecting malicious nodes reporting false data in a hierarchical sensor network. They employed a weighted trust evaluation (WTE in this paper) to make a decision on the correctness of the reports. The weights assigned to sensor nodes are updated after each cycle by reflecting the ratio of the number of incorrectly reporting nodes to the total number of nodes. Ju et al. [20] proposed an improved scheme based on WTE, named weighted-trust application (WTA). The weight of each sensor node is updated based on the behavior of the node itself.

Both WTE and WTA reduce the weights and normalize them after each cycle to keep the values in the range from 0 to 1. In the worst case, however, malicious nodes are likely to be detected with sacrificing some normal nodes. The loss of normal nodes might be problematic due to the resulting lack of network connectivity and sensing coverage. In addition, faults are only partially ta- ken into account in detecting malicious nodes. Consequently, both schemes might not achieve the expected performance in a sensor network where noise, natural faults, and malicious nodes coexist.

In this paper, we propose a dual weighted trust evaluation (DWE) scheme to detect malicious nodes in the face of faults in a hierarchical sensor network, where sensor nodes report their readings to a forwarding node for aggregation. Each sensor node is assigned two trust values. They are increased or decreased depending on its reading and the aggregation result at the forwarding node. An efficient updating policy is developed to keep mis-detection rate low while achieving high malicious node detection rate for a wide range of fault and related probabilities. Moreover, event detection accuracy and false alarm rate are also taken into account to be practically useful.

2. Network Model and Fault Model

The proposed scheme is also based on a three-layer hierarchical network architecture shown in Figure 1 [19].

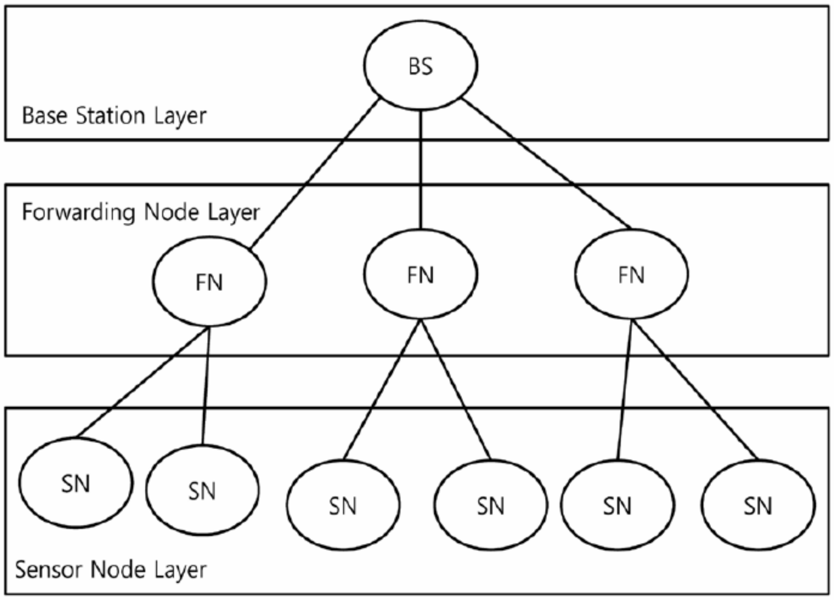

Fig: 1 A hierarchical sensor network

The above architecture is only for comparison purposes, where SN, FN, and BS represent the corresponding layers, respectively. Sensor nodes in SN (sensor node) layer are grouped, and the member nodes in each group directly communicate with the corresponding forwarding node in FN (forwarding node) layer to provide their sensor readings. Sensor nodes in SN layer are densely deployed to monitor the network area. They have limited power, memory, and computational capabilities. Sensor readings are assumed to be binary, 0 and 1 (alarm), and reported to the FN node. Nodes in FN layer are assumed to be more powerful as far as resources are concerned, and thus more dependable.

3. Performance Evaluation:

Computer simulation is conducted to evaluate the performance of the proposed malicious node detection scheme in a hierarchical sensor network, where 20 sensor nodes are under the control of a single forwarding node. Faults and malicious nodes are generated in accordance with predefined probabilities, pt (transient fault), pp (permanent fault), and pm (malicious node). In the case of permanent faults, both stuck-at-0 and stuck-at-1 are assumed to occur with the same probability. If pt = 0.2, for example, normal nodes are expected to report incorrect readings with a probability of 0.2. If pp = 0.1, both stuck-at-1 and stuck-at-0 occur with probability of 0.05 each. Malicious nodes are randomly generated with probability pm. They are assumed to report opposite to the sensor readings with probability pinv.

Four metrics, malicious node detection rate (MDR), misdetection rate (MR), false alarm rate (FAR), and event detection accuracy (EDA), are defined to show the effectiveness of our scheme compared to the existing WTA and WTE, although they focus only on malicious node detection. MDR is defined to be the ratio between the number of detected malicious nodes and the total number of existing malicious nodes. MR is defined to be the ratio between the number of normal nodes determined to be faulty and the total number of normal nodes. FAR is de- fined as the ratio of the number of no-event cycles with E = 1 to the total number of no-event cycles. Lastly, EDA is the ratio of the number of event cycles with E = 1 to the total number of event cycles.

In our scheme, if necessary, each sensor node can be logically removed from the network when its weight is less than or equal to Wlow. Sensor nodes excluded may optionally join the aggregation process later if their weights reach Whigh. If Wlow = 0 and Whigh = 1, for example, suspicious nodes are detected when their weights reach 0. Sensor nodes can be reinstated if their weights increase up to 1 (i.e., Whigh).

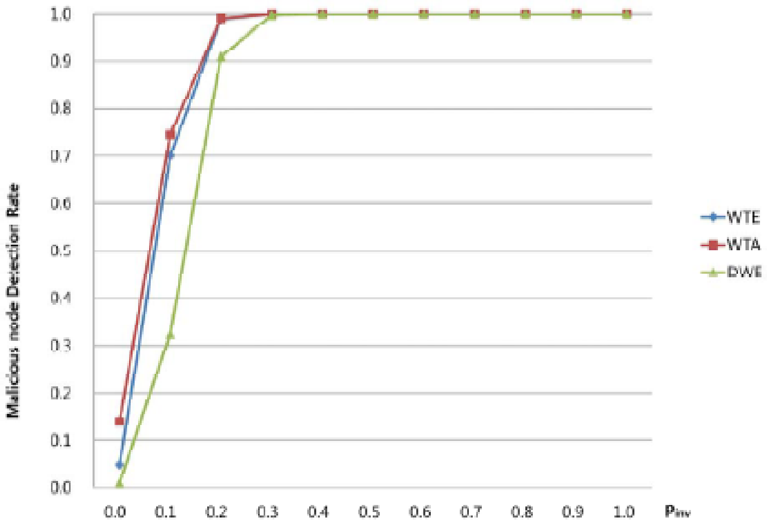

Fig: 2 MDR for various values of pinv.

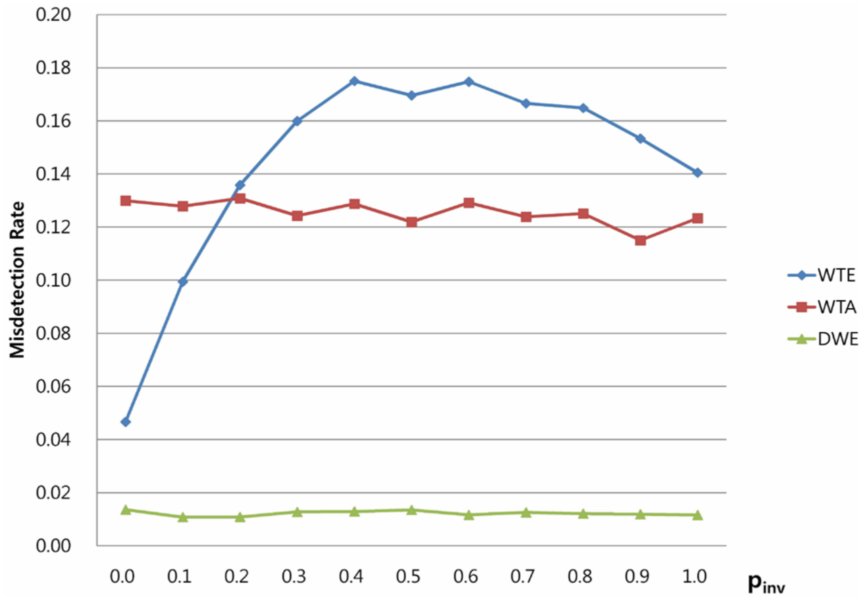

Fig: 3 MR for various values of pinv

Conclusion:

In this paper, we proposed a malicious and malfunctioning node detection scheme using dual weighted trust evaluation in a hierarchical sensor network. Malicious nodes are detected in the face of faults and noise by using a weighted majority voting. Trust values of sensor nodes are used as weights at the forwarding node to reflect the close to 1, while malicious nodes behaving differently from normal nodes gradually lose the weights to be detected. Implementing the scheme does not sacrifice nor-mal nodes even for high fault probabilities. The scheme is presented using a simple hierarchical model for convenience. The simulation is also limited for comparison with some existing schemes. It, however, is developed for more realistic sensor networks, and can thus be ap-plied to different structures without significant modifications.

References:

[1] S. Rajasegarar, C. Leckie and M. Palaniswami, "Anomaly Detection in Wireless Sensor Networks," IEEE Wireless Communications, Vol. 15, No. 4, 2008, pp. 34-40. doi:10.1109/MWC.2008.4599219

[2] M. Yu, H. Mokhtar and M. Merabti, "Fault Management in Wireless Sensor Networks," IEEE Wireless Sensor Net- working, Vol. 14, No. 6, 2007, pp. 13-19.

[3] B. Krishnamachari and S. Iyengar, "Bayesian Algorithms for Fault-tolerant Event Region Detection in Wireless Sensor Networks," IEEE Transactions on Computers, Vol. 53, No. 3, 2004, pp. 245-250. doi:10.1109/TC.2004.1261832

[4] T. Clouqueur, K. K. Saluja and P. Ramanathan, "Fault Tolerance in Collaborative Sensor Networks for Target Detection," IEEE Transactions on Computers, Vol. 53,

No. 3, 2004, pp. 320-333. doi:10.1109/TC.2004.1261838

[5] M. Ding, D. Chen, K. Xing and X. Cheng, "Localized Fault-Tolerant Event Boundary Detection in Sensor Net- works," 24th Annual Joint Conference of the IEEE Com- puter and Communications Societies, Miami, 13-17 March 2005, pp. 902-913.

[6] X. Luo, M. Dong and Y. Huang, "On Distributed Fault- Tolerant Detection in Wireless Sensor Networks," IEEE Transactions on Computers, Vol. 55 No. 1, 2006, pp. 58- 70. doi:10.1109/TC.2006.13

[7] C.-R. Li and C.-K. Liang, "A Fault-Tolerant Event Boun- dary Detection Algorithm in Sensor Networks," Informa- tion Networking: Towards Ubiquitous Networking and Services, Vol. 5200, 2008, pp. 406-414.

[8] X. Xu, B. Zhou and J. Wan, "Tree Topology Based Fault Diagnosis in Wireless Sensor Networks," International Conference on Wireless Networks and Information Sys- tems, Shanghai, 28-29 December 2009, pp. 65-69.

[9] M. H. Lee and Y.-H. Choi, "Fault Detection of Wireless Sensor Networks," Computer Communications, Vol. 31, No. 14, 2008, pp. 3469-3475. doi:10.1016/j.comcom.2008.06.014

[10] Y. Wang, G. Attebury and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Com- munications Surveys, Vol. 8, No. 2, 2006, pp. 2-23. doi:10.1109/COMST.2006.315852

[11] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attack and Countermeasures," Journal of Ad Hoc Networks, Vol. 1, No. 2-3, 2003, pp. 293-315.

[12] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defense," Third International Symposium on Information Processing in Sensor Networks, Berkeley, 26-27 April 2004, pp. 259- 268.

[13] Y. Hu, A. Perrig and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, San Francisco, 30 March-3 April 2003, pp. 1976-1986.

[14] B. Sun, K. Wu and U. Pooch, "Secure Routing against Black-Hole Attack in Mobile Ad Hoc Networks," Inter- national Conference on Communications and Computer Networks, Cambridge, 4-6 November 2002.

[15] W. Du, L. Fang and P. Ning, “LAD: Localization Ano- maly Detection for Wireless Sensor Networks,” 19th In- ternational Parallel and Distributed Processing Sympo- sium, Denver, 4-8 April 2005, p. 41.

[16] D. I. Curiac, O. Banias, F. Dragan, C. Volosencu and O. Dranga, “Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique,” 3rd In- ternational Conference on Networking and Services, Ath- ens, 19-25 June 2007, p. 83.

[17] W. Junior, T. Figueiredo, H. Wong and A. Loureiro, “Ma- licious Node Detection in Wireless Sensor Networks,” 18th International Parallel and Distributed Processing Sym- posium, Santa Fe, 26-30 April 2004, p. 24.

[18] M. Momani and S. Challa, “Survey of Trust Models in Different Network Domain,” International Journal Ad Hoc, Sensor & Ubiquitous Computing, 2010.

[19] I. M. Atakli, H. Hu, Y. Chen, W.-S. Ku and Z. Su, “Malicious Node Detection in Wireless Sensor Networks Using Weighted Trust Evaluation,” Proceedings of Spring Simu- lation Multiconference, Ottawa, 14-17 April 2008, pp. 836-843.

[20] L. Ju, H. Li, Y. Liu, W. Xue, K. Li and Z. Chi, “An Improved Intrusion Detection Scheme Based on Weighted Trust Evaluation for Wireless Sensor Networks,” Proceedings of the 5th International Conference on Ubiquitous Information Technology and Applications (CUTE), Sanya, 16-18 December 2010, pp. 1-6.