A Review on Wireless Sensor Network

Rohit Tripathi, Associate Professor, Department of Electronics, Electrical and Communications, Galgotias University

ABSTRACT

Wireless sensor networks' unsupervised nature renders them susceptible to malicious assaults. Hence, preserving safe data gathering is a key challenge for wireless sensor networks. We present a unique way to secure data collecting for wireless sensor networks. We examine secret sharing and multi-path routing with compromised nodes to secure data collecting in wireless sensor network. We describe a new tracing-feedback technique that takes full advantage of wireless sensor network routing features to increase data gathering quality. The main benefit this method is that secure pathways are developed as a data collecting by-product. Secure routing approach generates negligible overhead for network sensor nodes. Compared to prior research, the new approach algorithms are easily implemented and executed in resource-constrained wireless sensor networks. According to a simulation experiment, the approach's performance is superior than previous techniques with a similar aim.

Keywords: WSN, Approach, Simulation

INTRODUCTION

While intrusion detection is an essential problem for wireless sensor networks (WSNs), it is still in its infancy, and there are presently just a few research in this field. Due to WSN's fundamental properties, effective intrusion detection in such a resource-restricted setting is difficult[1]. Many Smart, statistical methodologies are too sophisticated for resource-constrained WSNs. Conversely, evading or bypassing rogue nodes is significantly simpler than detecting them. One proposed answer to such assaults is using WSN's routing capability. If the locations of the malicious nodes (also called compromised nodes) are known a priori, sensing information may be provided whenever feasible through pathways that circumvent (bypass) dangerous nodes. Since the present WSN intrusion detection systems are still immature, accurately acquiring such location information is problematic in practise. Therefore, the aforementioned principle is commonly implemented in a probabilistic approach. Multipath routing offers numerous pathways between one source and single destination node. It is often advocated to boost data transmission reliability (i.e., fault tolerance) or load balancing[2]. If the position information of compromised nodes is not known a priori, the source node may provide sensed information via different pathways to lessen the likelihood of interception.

Multipath Routing

Multipath routing technique, however, still has issues. Though the opponent can selectively compromise sensor nodes, detected information is intercepted in each fixed routing path, even if it may be dispersed over various routes. One alternative option is to provide information randomly via various ways rather than a predefined set of routes[3]. Although an adversary may still intercept portion of the information, employing precise procedures, we may minimise the likelihood of interception to an acceptable degree.

Secure Data Collection

There has been some ongoing research on multi-path routing for secure data collecting published in literature. For example, the SPREAD method in [4] is utilised to identify several safe and node-disjoint pathways. Using a modified Dijkstra method, repeatedly finds the top-K most secure node-disjoint pathways. The H-SPREAD algorithm[5] enhances the SPREAD algorithm by concurrently accounting for safety and reliability criteria. The work in [6] offers distributed Bound-Control and Lex-Control algorithms, computing numerous pathways. Shu et al. in[3] introduced a secure data gathering technique employing a (t, n)-threshold secret sharing method and randomised multi-path routes. A packet is split into shares, routed to the sink by randomly created pathways. They employ a fixed source node to test the simulation methodology while extending their simulation using a collection of source nodes. In [7], Nasser and Chen present a routing system that alternatively employs multipath as the path between two nodes. The protocol protects against certain attacks such as selective forwarding by presenting an appealing path to destination. In[8], Deng et al. offer an intrusion-tolerant WSN routing scheme. They strive to safeguard WSN security in one manner

Hash chains, layered message authentication codes, and multi-path routing. Yao et al. introduced WSN's multi-path secure routing protocol in[9-14]. However, their technique demands recognition of each node in routing. Therefore, the WSN's data collecting will generate substantial overhead.

Compared to earlier efforts in this sector, our solution uses a new tracing-feedback system that takes full advantage of WSN's routing ability to increase data collecting quality. Here, secure channels are theoretically safe for data collecting. Therefore, routing using secure pathways is more safer than multi-path routing. The main distinction between our technique and previous multi-path approaches is that the process of building secure pathways produces low overhead for sensor nodes, and the algorithms are straightforward to design and execute in resource-bound WSNs [15-18].

Conclusion

Embedded computer, sensor and integrated circuits make it feasible to construct large-scale networks with hundreds and thousands of extremely tiny, low-cost, battery-powered and wirelessly linked sensor and actuator nodes. Wireless sensor networks (WSNs) can work unattended for long periods and find a wide range of applications in the fields of environmental monitoring, forest fireproofing, habitat monitoring and control, smart agriculture, smart architecture and houses, defending military targets, preventing terror attacks, individual health monitoring, etc. [19].

Imagine a sensor network dispersed throughout a huge facility or region like a forest or battlefield[20]. Typical tasks for such networks are to send a message to a node at a given location, even without knowing how many nodes there are or how to reach them, to retrieve sensor data (e.g. sound, light, radiation, temperature or humidity) from nodes in a given region, and to use sensor nodes to track nearby events such as vehicles moving through the sensor field. Most of these activities involve knowing nodes' locations, or at least their relative locations. For example, for a vehicle-tracking application, sensor nodes would calculate tracked vehicle locations relative to their own locations.

REFERENCES

1. Barsan, N., Koziej, D., & Weimar, U. (2007). Metal oxide-based gas sensor research: How to? *Sensors and Actuators, B: Chemical*, *121*(1), 18–35. https://doi.org/10.1016/j.snb.2006.09.047

2. Bergveld, P. (2003). Thirty years of ISFETOLOGY: What happened in the past 30 years and what may happen in the next 30 years. *Sensors and Actuators, B: Chemical*, *88*(1), 1–20. https://doi.org/10.1016/S0925-4005(02)00301-5

3. Buettner, M., Yee, G. V, Anderson, E., & Han, R. (2006). X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks. *SenSys'06: Proceedings of the Fourth International Conference on Embedded Networked Sensor Systems*, 307–320. https://doi.org/10.1145/1182807.1182838

4. Ganeriwal, S., Kumar, R., & Srivastava, M. B. (2003). Timing-sync protocol for sensor networks. *SenSys'03: Proceedings of the First International Conference on Embedded Networked Sensor Systems*, 138–149. https://doi.org/10.1145/958507.958508

5. Grieshaber, D., MacKenzie, R., Vörös, J., & Reimhult, E. (2008). Electrochemical biosensors - Sensor principles and architectures. *Sensors*, *8*(3), 1400–1458. https://doi.org/10.3390/s8031400

6. Karl, H., & Willig, A. (2006). Protocols and Architectures for Wireless Sensor Networks. In *Protocols and Architectures for Wireless Sensor Networks*. wiley. https://doi.org/10.1002/0470095121

7. Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: A link layer security architecture for wireless sensor networks. *SenSys'04 - Proceedings of the Second International Conference on Embedded Networked Sensor Systems*, 162–175. https://www.scopus.com/inward/record.uri?eid=2-s2.0-26444574670&partnerID=40&md5=c8777ce91182ec4011567e35ef901bf7

8. Khoshelham, K., & Elberink, S. O. (2012). Accuracy and resolution of kinect depth data for indoor mapping applications. *Sensors*, *12*(2), 1437–1454. https://doi.org/10.3390/s120201437

9. Kim, H.-J., & Lee, J.-H. (2014). Highly sensitive and selective gas sensors using p-type oxide semiconductors: Overview. *Sensors and Actuators, B: Chemical*, *192*, 607–627. https://doi.org/10.1016/j.snb.2013.11.005

10. Lee, J.-H. (2009). Gas sensors using hierarchical and hollow oxide nanostructures: Overview. *Sensors and Actuators, B: Chemical*, *140*(1), 319–336. https://doi.org/10.1016/j.snb.2009.04.026

11. Levis, P., Lee, N., Welsh, M., & Culler, D. (2003). TOSSIM: Accurate and scalable simulation of entire TinyOS applications. *SenSys'03: Proceedings of the First International Conference on*

Embedded Networked Sensor Systems, 126–137. https://www.scopus.com/inward/record.uri?eid=2-s2.0-18844399081&partnerID=40&md5=f9423a6421cd539b3a6f7fc5f6eea902

12. Mainwaring, A., Polastre, J., Szewczyk, R., Culler, D., & Anderson, J. (2002). Wireless sensor networks for habitat monitoring. In S. K. M. Raghavendra C.S. (Ed.), *Proceedings of the ACM International Workshop on Wireless Sensor Networks and Applications* (pp. 88–97). Association for Computing Machinery (ACM). https://doi.org/10.1145/570748.570751

13. Maróti, M., Kusy, B., Simon, G., & Lédeczi, Á. (2004). The flooding time synchronization protocol. *SenSys'04 - Proceedings of the Second International Conference on Embedded Networked Sensor Systems*, 39–49. https://www.scopus.com/inward/record.uri?eid=2-s2.0-27644533289&partnerID=40&md5=6c6eb8ef24c305da9d864706607cdca6

14. Polastre, J., Hill, J., & Culler, D. (2004). Versatile low power media access for wireless sensor networks. *SenSys'04 - Proceedings of the Second International Conference on Embedded Networked Sensor Systems*, 95–107. https://doi.org/10.1145/1031495.1031508

15. Polastre, J., Szewczyk, R., & Culler, D. (2005). Telos: Enabling ultra-low power wireless research. *2005 4th International Symposium on Information Processing in Sensor Networks, IPSN 2005*, *2005*, 364–369. https://doi.org/10.1109/IPSN.2005.1440950

16. Stoppa, M., & Chiolerio, A. (2014). Wearable electronics and smart textiles: A critical review. *Sensors (Switzerland)*, *14*(7), 11957–11992. https://doi.org/10.3390/s140711957

17. Timmer, B., Olthuis, W., & Van Den Berg, A. (2005). Ammonia sensors and their applications - A review. *Sensors and Actuators, B: Chemical*, *107*(2), 666–677. https://doi.org/10.1016/j.snb.2004.11.054

18. Van Dam, T., & Langendoen, K. (2003). An adaptive energy-efficient MAC protocol for wireless sensor networks. *SenSys'03: Proceedings of the First International Conference on Embedded Networked Sensor Systems*, 171–180. https://doi.org/10.1145/958491.958512

19. Wang, C., Yin, L., Zhang, L., Xiang, D., & Gao, R. (2010). Metal oxide gas sensors: Sensitivity and influencing factors. *Sensors*, *10*(3), 2088–2106. https://doi.org/10.3390/s100302088

20. Woo, A., Tong, T., & Culler, D. (2003). Taming the underlying challenges of reliable multihop routing in sensor networks. *SenSys'03: Proceedings of the First International Conference on Embedded Networked Sensor Systems*, 14–27. https://doi.org/10.1145/958491.958494