Secure And Efficient Node Capture Attacks Using Dispersed Data Transmission For Wireless Sensor Networks

G.Kesavan, and N.V.Chinnasamy.

Abstract - Assurance networks are one of the essential technologies of New-generation Networks. Assurance is defined as the capability of guaranteeing functional and non-functional system properties such as dependability, security, timeliness and adaptability to heterogeneous and changing requirements. Assurance is essential for sustainable networks and this research focused specifically on providing assurance for WSNs. Node capture attacks are one prospective kind of attack on WSNs. To reduce negative effect of node capture attacks, we have previously proposed secure decentralized data transfer. In this proposed method, it was assumed that multiple paths were in place. In this paper as well, we again propose using the multipath routing method. To make multiple paths fit our previously proposed method; we have modified ATR (Augmented Tree Based Routing). We have conducted simulation experiments using our proposed method in a network simulator. The results show that our previously proposed method is effective in both cases in which the network size is small or large. In addition, we conducted other simulation experiments to measure several aspects of the assurance of our method. We measured in terms of varying parameters such as node densities, distance between the source and the destination nodes, and so on. Additionally, our method is more assured than the single path-based method.

Keywords:
Wireless Sensor Networks; Node Capture Attacks; Multipath Routing; Assurance; Socket Connection

I.INTRODUCTION

Wireless sensor networks (WSNs) are an important direction for future networks. Disaster response, weather observation, crime prevention, and healthcare systems are examples of applications where WSNs are utilized. The size of WSNs varies a great deal depending on the usage. WSNs consist of tiny nodes and sink nodes. Data on WSNs are transferred by wireless links. When a node (a source node) cannot communicate with the sink node (the destination node), intermediate nodes relay data from the source to the destination. This act of relaying data is referred to as multi-hop communication. Tiny nodes are deployed on the object or in the field to collect measurements. Because the nodes are small they have severely limited memory size and computational power. They are deployed in a possibly hostile environment in which several kinds of attacks may occur. Node capture attacks are one prospective kind of attack on WSNs. To prevent such attacks, several existing methods have been proposed.

TinySec is a security architecture used to ensure confidentiality when transferring data. TinySec uses a symmetric key such as RC4. While TinySec can protect data using key based cryptography, it is weak against node capture attacks. When a node is captured, adversaries can get the key of the cryptosystem and all of the data of the node. Since TinySec uses one common key for the system, adversaries can get all of the data in the network using the stolen key. To counter this, asymmetric key-based systems have been proposed. They are effective in limiting damage against attacks. When a secret key is captured in symmetric key-based and asymmetric key-based systems, those systems have to change the pair of keys. To do that, a random key pre-distribution scheme and its success or have been proposed. Those systems need to send control packets to create keys. These results in a large delay before data can be transmitted. That waiting time becomes long in large networks.

We have proposed a new method to protect data security against node capture attacks using distributed data transfer. To use this method, we have to establish multiple paths. In the past we proposed a scalable method to create multiple paths for distributed data transfer with a small number of control packets. In that same paper, we implemented the proposed method in the simulator by conducting simulation experiments on small and large networks and confirmed the effectiveness of the method on both. This proposed method was designed to hold up against changing environmental parameters such as the node density, the number of source nodes, and the hop length between sources and the destination. In real systems, the resiliency in light of those varying parameters will be important. *Assurance* or *assurance networks* express that resiliency.

G.Kesavan,Research Scholar in M.Phil,Sri Vijay Vidyalaya College of Arts and Science, Dharmapuri.
N.V.Chinnasamy, Assistant Professor, Department of Computer Science,
Sri Vijay Vidyalaya College of Arts and Science, Dharmapuri.

kesavansevan.7@gmail.com

According to, assurance in distributed systems and networks is defined as the capability of guaranteeing functional and on-functional system properties such as dependability, security, timeliness and adaptability to heterogeneous and changing requirements. Networks which have the aforementioned assurance are defined as *assurance networks*. Assurance network technologies are important for *New-generation networks*, which Japan's National Institute of Information and Communication Technology plans to research. In the literature, Avižienis et al. proposed the concept of dependability. They claimed that simultaneous consideration of dependability and security provides a very convenient means of subsuming various concerns within a single conceptual framework. Assurance is one framework that looks into faults and security. In this paper, we propose a method to evaluate both the security aspect of assurance, by focusing on confidentiality, and the dependability aspect, by focusing on resiliency against node faults.

II.RELATED WORK

In wireless sensor networks (WSNs), tiny sensor nodes are deployed on the object or to the field to collect measurements. A tiny sensor node has limited resources such as the available CPU power and the memory size.

In addition, the field to be measured is a possibly hostile environment for WSNs in many cases. The tiny sensor nodes are deployed and work autonomously for a certain period of time. It is not feasible for each sensor node to have detecting capabilities to sense adversaries. To cope with security problems in WSNs, many countermeasures have been proposed.

Although many of them are key-based systems, the protection of the secret key(s) is a serious concern. When secret keys are stolen by way of node capture attacks, encrypted data can be decrypted by adversaries. In the past, we have proposed a method to secure decentralized data transfer against node capture attacks (hereafter referred to as the previously proposed method). Fig. 1 shows the data transfer of our previously proposed method. The previously proposed method can encrypt data being transferred using the secret-sharing-scheme-based data dispersion. In the literature, we can confirm the effectiveness of our previously proposed method using small size networks consisting of about nine nodes.

Assurance in these distributed systems and networks is defined as the capability of guaranteeing functional and nonfunctional system properties such as dependability, security, timeliness and adaptability to heterogeneous and changing requirements. To ensure the security in WSNs, it is important to consider what different scales of networks require. An approach to assurance in WSN security is to apply multipath routing required in our previously proposed method to the currently proposed method.

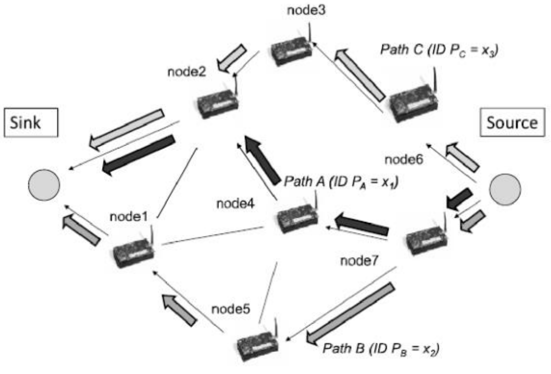


Fig 1: Dispersed Data Transmission in WSN

III.DISPERSED DATA TRANSIMISSION FOR WIRELESS SENSOR NETWORKS

3.1 Data Integrity

Although data confidentiality guarantees that only intended parties obtain the un-encrypted plain data, it does not protect data from being altered. Data integrity guarantees that a message being transferred is never corrupted. A malicious node may just corrupt messages to prevent network from functioning properly. In fact, due to unreliable communication channels, data may be altered without the presence of an intruder. Thus, message authentication codes or cyclic codes are used to prevent data integrity. Data aggregation results in alterations of data; therefore, it is not aggregation is employed. Moreover, if a data aggregator is compromised, then it may corrupt sensor data during data aggregation and the base station has no way of checking the integrity of this aggregated sensor data. Providing data integrity is not enough for wireless communication because compromised sensor nodes are able to listen to transmitted messages and replay them later on to disrupt the data aggregation results. Data freshness protects data aggregation schemes against replay attacks by ensuring that the transmitted data is recent.

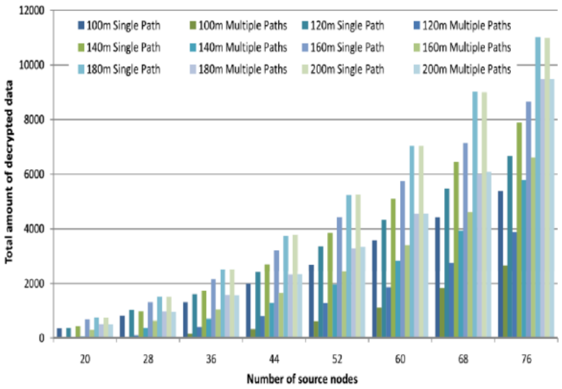
3.2 Source Security

Since wireless sensor networks use a shared wireless medium, sensor nodes need DSP mechanisms to detect maliciously injected or spoofed packets. Source authentication enables a sensor node to ensure the identity of the peer node it is communicating with. Without source authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Moreover, a compromised node may send data to its data aggregator under several fake identities so that the integrity of the aggregated data is corrupted. Faking multiple sensor node identities is called Sybil attack and it poses significant threat to data aggregation protocols. If only two nodes are communicating, authentication can be provided by DSP. The sender and the receiver share a secret key to compute the message authentication code (MAC) for all transmitted data.

3.3 Data Aggregation

Since wireless sensor networks use a shared wireless medium, sensor nodes need DSP mechanisms to detect maliciously injected or spoofed packets. Source authentication enables a sensor node to ensure the identity of the peer node it is communicating with. Without source authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Moreover, a compromised node may send data to its data aggregator under several fake identities so that the integrity of the aggregated data is corrupted. Faking multiple sensor node identities is called Sybil attack and it poses significant threat to data aggregation protocols. If only two nodes are communicating, authentication can be provided by DSP. The sender and the receiver share a secret key to compute the message authentication code (MAC) for all transmitted data. protocols. Earlier work on data aggregation focused on improving the existing routing algorithms so as to make data aggregation possible. As a result, many data aggregation protocols based on shortest path tree structure have been proposed. To reduce the latency due to tree-based data aggregation, recent work on data aggregation tends to group sensor nodes into clusters so that data are aggregated in each group for improved efficiency.

3.4 Simulation Results



IV.CONCLUSION

In this paper, we have proposed multipath routing as an extension of our previously proposed method of data dispersal. To make multiple paths fit our previously proposed method, we modified ATR. We have conducted simulation experiments using our proposed method in a network simulator. The results show that our proposed method is effective in both cases in which the network size is small and large. In addition, we conducted other simulation experiments to measure several aspects of the assurance of our method. We measured in terms of varying parameters such as node densities, distance between the source and the destination nodes, and so on. Additionally, our method is more assured than the single path based method.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: A survey, Comput. Netw. 38 (4) (2002) 393–422.

[2] I. Stojmenovi'c (Ed.), Handbook of Sensor Networks: Algorithms and Architectures, Wiley, 2005.

[3] W. Zhang, S.K. Das, Y. Liu, Security in wireless sensor networks: A survey, in: Y. Xiao (Ed.), Security in Sensor Networks, Auerbach Publications, 2007,
pp. 237–272.

[4] C. Karlof, N. Sastry, D. Wagner, TinySec: a link layer security architecture for wireless sensor networks, in: SenSys'04: Proceedings of the 2nd International
Conference on Embedded Networked Sensor Systems, ACM, New York, NY, USA, 2004, pp. 162–175, http://doi.acm.org/10.1145/1031495.1031515.

[5] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: CCS'02: Proceedings of the 9th ACM Conference on Computer and Communications Security, ACM, New York, NY, USA, 2002, pp. 41–47, http://doi.acm.org/10.1145/586110.586117.

[6] W. Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, A. Khalili, A pairwise key predistribution scheme for wireless sensor networks, ACM Transactions on Information and System Security (TISSEC) 8 (2) (2005) 228–258, http://doi.acm.org/10.1145/1065545.1065548.

[7] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, in: Proceedings of the 2003 IEEE Symposium on Security and Privacy, Oakland, California, USA, 2003, pp. 197–213.

[8] E. Kohno, T. Ohta, Y. Kakuda, M. Aida, Improvement of dependability against node capture attacks for wireless sensor networks, IEICE Trans. Inf. Syst. E94-D (1) (2011) 19–26.

[9] E. Kohno, T. Okazaki, M. Takeuchi, T. Ohta, Y. Kakuda, M. Aida, Improvement of the security against node capture attacks using dispersed data transmission for wireless sensor networks, in: Proc. Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing (UIC-ATC 2010), Xi'an, PR China, 2010, pp. 340–345.

[10] Y. Kakuda, Assurance networks: Concepts, technologies, and case studies, in: Proc. 7th Int Ubiquitous Intelligence & Computing and 7th Int. Conf. Autonomic & Trusted Computing (UIC/ATC) Conf., 2010, pp. 311–315, doi:10.1109/UIC-ATC.2010.33.

[11] A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, IEEE Transactions on Dependable and Secure Computing 1 (1) (2004) 11–33, doi:10.1109/TDSC.2004.2.

[12] E. Kohno, T. Ohta, Y. Kakuda, Secure decentralized data transfer against node capture attacks for wireless sensor networks, in: Proceedings of the 9th IEEE International Symposium on Autonomous Decentralized Systems (ISADS 2009), Athens, Greece, 2009, pp. 35–40.

[13] A. Shamir, How to share a secret, Commun. ACM 22 (1979) 612–613, http://doi.acm.org/10.1145/359168.359176.

[14] E.D. Karnin, J.W. Greene, M.E. Hellman, On secret sharing systems, IEEE Trans. Inform. Theory IT-29 (1) (1983) 35–41.

[15] M. Caleffi, G. Ferraiuolo, L. Paura, Augmented tree-based routing protocol for scalable ad hoc networks, in: Proceedings of the Third IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS'07), IEEE Computer Society, Los Alamitos, CA, USA, 2007, pp. 1–6, http://doi.ieeecomputersociety.org/10.1109/MOBHOC.2007.4428727.

[16] J. Eriksson, M. Faloutsos, S.V. Krishnamurthy, DART: Dynamic address routing for scalable ad hoc and mesh networks, IEEE/ACM Trans. Netw. 15 (1) (2007) 119–132.

[17] T. Okazaki, E. Kohno, T. Ohta, Y. Kakuda, A multipath routing method with dynamic ID for reduction of routing load in ad hoc networks, in: J. Zheng, D. Simplot-Ryl, V.C.M. Leung (Eds.), ADHOCNETS'10, in: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 49, 2010, pp. 114–129.

[18] Scalable Network Technologies, Inc., QualNet network simulator, http://www.scalable-networks.com/.

[19] L.P. Deutsch, RFC 1952: GZIP file format specification version 4.3, status: INFORMATIONAL, May 1996, ftp://ftp.internic.net/rfc/rfc1952.txt, ftp://ftp.math.utah.edu/pub/rfc/rfc1952.txt.

[20] M. Ishizuka, M. Aida, Achieving power-law placement in wireless sensor networks, in: Proceedings of the 7th IEEE International Symposium on Autonomous Decentralized Systems (ISADS 2005), 2005, pp. 661–666.