ISSN:0975-9646

False Node Detection in Trust Aware Routing Framework (TARF) in WSN

Bhagyashree N V
Dept. PGSCEA
The National Institute of Engineering
Mysore

Assoc Prof. Bhat Geetalaxmi Jairam
Dept.IS&E
The National Institute Of Engineering
Mysore

Abstract: In Wireless sensor networks (WSN), the wide range of communication is not that much secure when compared to limited area network. The multi-hop routing in wireless sensor networks (WSNs) offers little protection against identity deception through replaying routing information. Traditional cryptographic techniques or efforts at developing trust-aware routing protocols do not effectively address this severe problem. To secure the WSNs against adversaries misdirecting the multi-hop routing, we have designed and implemented a model to detect false node in TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception. With this to find the false node, we are designing two novel node clone detection techniques with different trade-offs on network conditions and performance security is provided. The first one is based on a distributed hash table (DHT), it is a fully decentralized, key-based caching and checking system is constructed to catch cloned or duplicated nodes effectively. Our second distributed detection protocol, named randomly directed exploration, the protocol is mainly designed to provide good communication performance in dense sensor networks, by a probabilistic directed forwarding technique along with random initial direction and border determination.

Keywords: Wireless sensor networks, routing protocols, security, DHT, clone attack, randomly directed exploration

I. INTRODUCTION

Wireless sensor networks (WSNs) [2] are ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire monitoring. A WSN comprises battery-powered sensor nodes with extremely limited processing capabilities. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multihop path. However, the multihop routing of WSNs of ten becomes the target of malicious attacks. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference [3].

This paper focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception, the adversary is capable of launching harmful and hard-to-detect attacks against routing, such as selective forwarding, wormhole attacks, sinkhole attacks and Sybil attacks [4]. As a harmful and easy-to-implement type of attack, a malicious node simply replays all the outgoing routing packets from a valid node to forge the latter node's identity; the malicious node then uses this forged identity to participate in the network routing, thus disrupting the network traffic. Those routing packets, including their original headers, are replayed without any modification. Even if this malicious node cannot directly overhear the valid node's wireless transmission, it can collude with other malicious nodes to receive those routing packets and replay them somewhere far away from the original valid node, which is known as a wormhole attack [5].

Since a node in a WSN usually relies solely on the packets received to know about the sender's identity, replaying routing packets allows the malicious node to forge the identity of this valid node. After "stealing" that valid identity, this malicious node is able to misdirect the network traffic. For instance, it may drop packets received, forward packets to another node not supposed to be in the routing path, or even form a transmission loop through which packets are passed among a few malicious nodes infinitely. It is often difficult to know whether a node forwards received packets correctly even with overhearing techniques [4]. Sinkhole attacks are another kind of attacks that can be launched after stealing a valid identity. In a sinkhole attack, a malicious node may claim itself to be a base station through replaying all the packets from a real base station [6]. Such a fake base station could lure more than half the traffic, creating a "black hole." This same technique can be employed to conduct another strong form of attack — Sybil attack [7]: through replaying the routing information of multiple legitimate nodes, an attacker may present multiple identities to the network. A valid node, if compromised, can also launch all these attacks. The harm of such malicious attacks based on the technique of replaying routing information is further aggravated by the introduction of mobility into WSNs and the hostile network condition. Though mobility is introduced into WSNs for efficient data collection and various applications [8], [9],[10],[11], it greatly increases the chance of interaction between the honest nodes and the attackers.

Additionally, a poor network connection causes much difficulty in distinguishing between an attacker and a honest node with transient failure. Without proper protection, WSNs with existing routing protocols can be completely devastated under certain circumstances. In an emergent sensing application through WSNs, saving the network from being devastated becomes crucial to the success of the application.

In this paper, we present two novel, practical node clone detection protocols with different trade-offs on network conditions and performance. The first proposal is based on a distributed hash table (DHT) [21], by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes. The protocol's performance on memory consumption and a critical security metric are theoretically deducted through a probability model, and the resulting equations, with necessary adjustment for real application, are supported by the simulations. In accordance with our analysis, the comprehensive simulation results show that the DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks. Our second protocol, named randomly directed exploration, is intended to provide highly efficient communication performance with adequate detection probability for dense sensor networks. In the protocol, initially nodes send claiming messages containing a neighbour-list along with a maximum hop limit to randomly selected neighbours; then, the subsequent message transmission is regulated by a probabilistic directed technique to approximately maintain a line property through the network as well as to incur sufficient randomness for better performance on communication and resilience against adversary.
In addition, border determination mechanism [22][23] is employed to further reduce communication payload. During forwarding, intermediate nodes explore claiming messages for node clone detection. By design, this protocol consumes almost minimal memory, and the simulations show that it outperforms all other detection protocols in terms of communication cost, while the detection probability is satisfactory.

II. LITERATURE SURVEY

2.1 Distributed detection node replication attacks in sensor networks

The low-cost, off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With little effort, an adversary may capture nodes, analyse and replicate them, and surreptitiously insert these replicas at strategic locations within the network. Such attacks may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighbourhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, we propose two new algorithms based on emergent properties (Gligor (2004)) [15], i.e., properties that arise only through the collective action of multiple nodes. Randomized multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, while line-selected multicast uses the topology of the network to detect replication. Both algorithms provide globally-aware, distributed node-replica detection, and line-selected multicast displays particularly strong performance characteristics. We show that emergent algorithms represent a promising new approach to sensor network security; moreover, our results naturally extend to other classes of networks in which nodes can be captured, replicated and re-inserted by an adversary.

2.2 Location-based compromise tolerant security mechanisms for wireless sensor networks

Node compromise is a serious threat to wireless sensor networks deployed in unattended and hostile environments. To mitigate the impact of compromised nodes, we propose a suite of location-based compromise-tolerant security mechanisms. Based on a new cryptographic concept called pairing, we propose the notion of location-based keys (LBKs) [18][19] by binding private keys of individual nodes to both their IDs and geographic locations. We then develop an LBK-based neighbourhood authentication scheme to localize the impact of compromised nodes to their vicinity. We also present efficient approaches to establish a shared key between any two network nodes. In contrast to previous key establishment solutions, our approaches feature nearly perfect resilience to node compromise, low communication and computation overhead, low memory requirements, and high network scalability. Moreover, we demonstrate the efficacy of LBKs in counteracting several notorious attacks against sensor networks such as the Sybil attack, the identity replication attack, and wormhole and sinkhole attacks. Finally, we propose a location-based threshold-endorsement scheme, called LTE, to thwart the infamous bogus data injection attack, in which adversaries inject lots of bogus data into the network. The utility of LTE in achieving remarkable energy savings is validated by detailed performance evaluation.

2.3 A survey on sensor networks

The advancement in wireless communications and electronics has enabled the development of low-cost sensor networks. The sensor networks can be used for various application areas (e.g., health, military, home). For different application areas, there are different technical issues that researchers are currently resolving. The current state of the art of sensor networks is captured in this article, where solutions are discussed under their related protocol stack layer sections. This article also points out the open research issues and intends to spark new interests and developments in this field.

2.4 Key infection: Smart trust forsmart dust

Future distributed systems may include large self-organizing networks of locally communicating sensor nodes, any small number of which may be subvened by an adversary. Providing security for these sensor networks is important, but the problem is complicated by the fact that managing cryptographic key material is hard: low-cost nodes are neither tamper-proof nor capable of performing public key cryptography efficiently. We show how the key distribution problem can be dealt with in environments with a partially present, passive adversary: a node wishing to communicate securely with other nodes simply generates a symmetric key[16] and sends it in the clear to its

neighbours. Despite the apparent insecurity of this primitive, we can use mechanisms for key updating, multipath secrecy amplification and multihop key propagation to build up extremely resilient trust networks where at most a fixed proportion of communications links can be eavesdropped. We discuss applications in which this assumption is sensible. Many systems must perforce cope with principals who are authenticated weakly, if at all; the resulting issues have often been left in the 'too hard' tray. One particular interest of sensor networks is that they present a sufficiently compact and tractable version of this problem. We can perform quantitative analyses and simulations of alternative strategies, some of which we present here. We also hope that this work may start to challenge the common belief that authentication is substantially about bootstrapping trust. We argue that, in distributed systems where the opponent can subvert any small proportion of nodes, it is more economical to invest in resilience than in bootstrapping.

III. CONCLUSION

Designed and implemented TARF, a robust trust aware routing framework for WSNs, to secure multihop routing in dynamic WSNs against harmful attackers exploiting the replay of routing information. TARF focuses on trustworthiness and energy efficiency, which are vital to the survival of a WSN in a hostile environment. With the idea of trust management, TARF enables a node to keep track of the trustworthiness of its neighbours and thus to select a reliable route.

Unlike previous efforts at secure routing for WSNs, TARF effectively protects WSNs from severe attacks through replaying routing information; it requires neither tight time synchronization nor known geographic information. The resilience and scalability of TARF are proved through both extensive simulation and empirical evaluation with large-scale WSNs; the evaluation involves static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks.

With this we present two distributed detection protocols: One is based on a distributed hash table, which forms a Chord overlay network and provides the key-based routing, caching, and checking facilities for clone detection, and the other uses probabilistic directed technique to achieve efficient communication overhead for satisfactory detection probability. While the DHT-based protocol provides high security level for all kinds of sensor networks by one deterministic witness and additional memory-efficient, probabilistic witnesses, the randomly directed exploration presents outstanding communication performance and minimal storage consumption for dense sensor networks.

REFERENCES

[1] G. Zhan, W. Shi, and J. Deng, "Tarf: A trust-aware routing framework for wireless sensor networks," in *Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10)*, 2010.

[2] F. Zhao and L. Guibas, *Wireless Sensor Networks: An Information Processing Approach*. Morgan Kaufmann Publishers, 2004.

[3] A. Wood and J. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct 2002.

[4] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[5] M. Jain and H. Kandwal, "A survey on complex wormhole attack in wireless ad hoc networks," in *Proceedings of International Conference on Advances in Computing, Control, and Telecommunication Technologies (ACT '09)*, 28-29 2009, pp. 555 –558.

[6] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side", *Proc. IEEE Int'l Conf. Wireless and Mobile Computing, Networkingand Comm. (WIMOB '08), pp. 526-531, 2008.*

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis and defenses," in *Proc. of the 3rd International Conference on Information Processing in Sensor Networks (IPSN'04)*, Apr. 2004.

[8] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, "Performance analysis of mobile agent-based wireless sensor network," in *Proceedings of the 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009)*, 20-24 2009, pp. 16 –19.

[9] L. Zhang, Q. Wang, and X. Shu, "A mobile-agent-based middleware for wireless sensor networks data fusion," in *Proceedings of Instrumentation and Measurement Technology Conference (I2MTC '09)*, 5-7 2009, pp. 378 –383.

[10] W. Xue, J. Aiguo, and W. Sheng, "Mobile agent based moving target methods in wireless sensor networks," in *IEEE International Symposium on Communications and Information Technology (ISCIT 2005)*, vol. 1, 12-14 2005, pp. 22 – 26.

[11] J. Hee-Jin, N. Choon-Sung, J. Yi-Seok, and S. Dong-Ryeol, "A mobile agent based leach in wireless sensor networks," in *Proceedings of the 10th International Conference on Advanced Communication Technology (ICACT 2008)*, vol. 1, 17-20 2008, pp. 75 –78.

[12] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: a survey," *Wireless Communications*, vol. 11, no. 6, pp. 6–28, Dec. 2004.

[13] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in *Proc. of ACM SenSys 2004*, Nov. 2004.

[14] A. Perrig, R. Szewczyk, W. Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," *Wireless Networks Journal (WINET)*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[15] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: securing sensor networks with public key technology," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04)*. New York, NY, USA: ACM, 2004, pp. 59–64.

[16] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Proceedings of the 7th international conference on Information processing in sensor networks (IPSN '08)*. IEEE Computer Society, 2008, pp. 245–256.

[17] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[18] H. Safa, H. Artail, and D. Tabet, "A cluster-based trust-aware routing protocol for mobile ad hoc networks," *Wirel. Netw.*, vol. 16, no. 4, pp. 969–984, 2010.

[19] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, and K. Lam, "Trust based routing for misbehavior detection in ad hoc networks," *Journal of Networks*, vol. 5, no. 5, May 2010.

[20] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," in *Proceeding of the 7th Nordic Workshop on Secure IT Systems*, 2003.

[21] B. Parno, A. Perrig, and V. Gligor, "Distributed detection node replication attacks in sensor networks," in *Proc. IEEE Symp. Security Privacy*, 2005, pp. 49–63

[22] Y. Zhang,W. Liu,W. Lou, and Y. Fang, "Location-based compromise tolerant security mechanisms for wireless sensor networks," *IEEE J.Sel. Areas Commun.*, vol. 24, no. 2, pp. 247–260, Feb. 2006.

[23] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in *Proc. 10th ACM CCS*, Washington, DC, 2003, pp. 62–72.

[24] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in *Proc. 3rd SecureComm*, 2007, pp. 341–350

[25] L. Eschenauer and V. D. Gligor, "A key-management scheme for

distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun.Security*, Washington, DC, 2002, pp. 41–47

[26] I. F. Akyildiz, W. Su, Y.Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp.102–114, Aug. 2002.

Smt. Bhat Geethalaxmi Jayaram is Associate Professor in the Department of Information Science & Engineering at NIE Mysore. She has received her M.Tech from VTU, and B.E. from Latur. She is pursuing her Ph.D. in Wireless Sensor Networks.

She has been awarded VGST Grant for establishing the facility for – Research work on "Energy efficient data gathering using multiple mobile elements in wireless sensor networks" to CS&E Dept., NIE.