International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume –04, Issue – 12, December 2019, PP – 05-08

A survey of Node Misbehaviour Attack and Node Capture Attack in Wireless Sensor Networks

[1]D.Jeyamani latha *M.E.Ph.D Scholar,*
Associate Professor,VITech,Panchetti-601204

[2]Dr. B. Diwan *M.E.Ph.D,*
Associate Professor, St. Joseph College of Engineering, Chennai

Abstract: For designing security protocols to achieve confidentiality, authentication, integrity and non-repudiation Cryptographic primitives are used. . There are a number of surveys on security issues on WSNs, which, however, did not focus on public-key cryptographic primitives in WSNs. In this survey, we provide a deeper understanding of public-key cryptographic primitives in WSNs including identity-based cryptography and discuss their main directions and some open research issues that can be further pursued. We investigate state-of-the-art software implementation results of public-key cryptographic primitives in terms of execution time, energy consumption and resource occupation on constrained wireless devices choosing popular IEEE 802.15.4-compliant WSN hardware platforms, used in real-life deployments.

Keyword: Identity-based cryptography, public-key cryptography, public-key encryption, side-channel attack, software implementation

I. Introduction

This survey provides invaluable insights on public-key cryptographic primitives on WSN platforms, and solutions to find tradeoffs between cost, performance and security for designing security protocols in WSNs.

In most of survey papers on WSNs, security issues are divided into from five to seven categories including cryptography, secure routing, secure data aggregation, secure data fusion, location security.

we target at side channel attacks (SCAs) which try to extract secret information from the physical implementation of cryptographic algorithms. Once mathematically strong cryptographic primitives are implemented in either software or hardware, they are known to be vulnerable to various physical attacks such as SCAs.

While a cryptographic device is performing cryptographic computations, an attacker can monitor the side channel information leakage, such as power consumption, timing, and electromagnetic emanations if nodes are captured or on the spot. Goal of SCAs is to extract a secret key of the implemented cryptographic algorithm from the physical behavior of the target device. The attacker may use techniques such as power analysis, execution cycle frequency analysis, timing information analysis (on data movement into and out of the CPU), electromagnetic radiation analysis, acoustic emission analysis, etc.

Kocher *et al.* [1] first presented power analysis attacks on Data Encryption Standard (DES) [2], in which an attacker determined a secret key of DES by measuring the power consumption of the algorithm running on a smart card. Almost all block ciphers including Advanced Encryption Standard (AES) [3], which is a current symmetric-key encryption standard of electronic data established by the National Institute of Standards and Technology (NIST) in 2002, are vulnerable to SCAs. Okeya and Iwata [4] showed that message authentication codes (MACs), EMAC, OMAC, and PMAC, are vulnerable to SPA or DPA.

a. Public-Key Cryptography

Cryptographic techniques are typically divided into two generic types: symmetric-key and public-key.

Symmetric-Key Cryptography

In this type of message encryption, sender and receiver only have to share the same secret key in the beginning and then they can begin to encrypt and decrypt messages between them using that key. This key predistribution process is very difficult. SKC cannot achieve non-repudiation, as both sender and receiver use the same key, messages cannot be verified to have come from a particular user.

SKC offers advantages in terms of low communication and computational overhead. One may believe that SKC is more suitable for WSN applications which requires only confidentiality or data integrity. To apply SKC to these WSNs, the shared-key distribution is needed. The key predistribution methods have the following three types:

- A single network-wise secret key: this causes a single point failure, i.e., if the secret key of a node is revealed then the entire network is broken.
- A pairwise key between a node and the BS or between two nodes:
- A group key among a set of nodes: group keying is more inefficient than the pairwise keying as it is required heavy computational overhead and interactions with more than two rounds among nodes.

Public-Key Encryption

The security of PKE schemes is usually classified from the point of view of their goals and attack models. The standard goals of PKE schemes are as follows:

•**Semantic Security** *(*SS*).* Any adversary (probabilistic polynomial-time Turing Machine) cannot obtain any partial information about the plaintext of a given ciphertext [5]. This notion corresponds to a computational version of perfect secrecy introduced by Shannon [6].

•**Indistinguishability** *(*IND*).* Given a ciphertext of one of two plaintexts, any adversary cannot distinguish which one is encrypted [5].

•**Non-malleability***(*NM*).*Given a ciphertext of a plaintext, any adversary cannot construct another ciphertext whose plaintext is meaningfully related to the initial one [7].

Semantic security, defined by Goldwasser and Micali [5],captures the intuition that an adversary should not be able toobtain any partial information about a message given its encryption.A different notion of security, called non-malleability ,was proposed by Dolev, Dwork, and Naor [7]. The adversary also has access to a decryption oracle, but its goal is notto obtain partial information about the plaintext of the target ciphertext but rather to create another encryption of a different message that is related in some interesting way to the original, encrypted message.

Public-Key Signatures

A public-key signature (PKS) or digital signature is a contrary concept of a PKE scheme: it signs on a message with a secret key and then its resulting signature is publicly verified with a public key corresponding the secret key. PKSs have many applications in information security, including authentication, data integrity, and non-repudiation. The PKS schemes can be the following two classes [8]:

- **Signature Schemes with Appendix**. It requires an original message as input to the verification algorithm.
- **Signature Schemes with Message Recovery**. It does not require an original message as input to the verification algorithm.

In this case, the original message is recovered from the signature itself.

II. Node Misbehaviour Attacks

In this chapter we are going to discuss with how to select an optimized route. here the routing decisions are based on trust, energy and hop count.

Stealth Jamming in adhoc networks

*Stealth Jamming (SJAM)*technique, target a relatively unexplored weakness inherent in the route maintenance mechanism of ***ad*** *hoc* protocols used by trust-aware routing schemes. Missing a certain number of transmission attempts at the data link layer is typically considered as the link, and consequently route breakage.

Trust and Energy-aware Routing Protocol (TERP) is proposed to deal with node misbehaviour attacks. TERP utilizes both direct and indirect trust for evaluating the trustworthiness of nodes. In order to select an optimized route, routing decisions are based on trust, energy and hop count. However, for reporting route breakages conventional route repair mechanism is employed.

Reputation-Aware AODV routing protocol (RAAODV) [9] is proposed to deal with the selfish behaviour of nodes, where they do not cooperate in packet forwarding to conserve their resources. The packet forwarding decisions are based on trust and hop counts. RAAODV makes use of redemption approach thereby allowing a malicious node to become part of the network once the redemption period expires.

A trust and QoS aware routing protocol TQR [10] is proposed for mobile ad-hoc networks to avoid black hole attack. A link quality metric, ETX along with trustworthiness of nodes is used to select routing paths. TQR evaluates the trustworthiness of nodes based on both direct and indirect trusts.

Trust Aware Routing Framework (TARF) [11] routing protocol has been proposed to safeguard against wormhole and other node misbehaviour attacks. An asymmetric authentication mechanism has been employed for verifying broadcast packets, which further requires a cryptographic algorithm and time synchronization for their operations.

These schemes do nothing to minimize route breakage notifications by evaluating actual status of the link based on channel interference. The significant interference may cause inconsistent decision making regarding actual route breakages, consequently impact on delay, throughput and link reliability performance.

The anti-jamming schemes, DEEJAM and Dodge-Jam, require some special resources such as tight-time synchronization, frequency-hopping and pre-shared keys thereby imposing constraints for network operations and results in high energy consumption and overheads. Moreover, these schemes consider the jamming behaviour at PHY and MAC layers, however, do not consider the jamming behaviour at routing layer.

Stealth Jamming Attack

The misbehaving nodes with jamming attack behaviour, intentionally strain the communication channels by introducing malicious/fake traffic to disrupt the on-going transmission .In this paper, we employ the stealth jamming attack behaviour where a jamming node randomly jams the traffic by sending-out fake/bogus radio signals and alternate between the jamming and sleep modes. After jamming the network traffic for certain periods of time, the jamming node turn off its radio and switches to sleep mode. After some time it resumes jamming behaviour. This makes stealth jamming attack difficult to detect due to its randomly changing behaviours.

The throughput experiences variations in the performance due to significant interference and route maintenance calls. Such transmission disruption affects the flow of data packets. Similarly, end-to-end delay also exhibits decreased performance as nodes have to waitto find new routes due to route breakage notification.

III. Node Capture Attack in Wireless Sensor Networks

In this chapter the inherent resource on straints of sensor nodes restrict using expensive security solutions for WSN. we present a novel approach of program integrity verification (PIV) protocol to detect whether a node is captured. The cluster head equipped with trusted platform module (TPM) verifies by comparing the program memory content of the sensor node before and after capture. The proposed TPIV protocol can detect the captured node even in the presence of a strong adversary capable of putting additional memory to elude the PIV.

Although researchers have addressed various aspects of WSN security such as secure key management, secure localization, and data aggregation [12], the problem of node capture attack is still a major concern in WSN. In a node capture attack, an attacker gets hold of a node physically and then reprograms and redeploys the node. The severity of the attack depends on the time and resources available with the attacker.

The node capture attack is critical to any WSN application; therefore, the need to efficiently and securely detect a captured node is a challenging research problem. In this paper, we present a protocol to detect the node capture attack in a clustered WSN using PIV. In the proposed TPM-enabled PIV (TPIV) protocol; each cluster head managing a group of nodes in the network is equipped with TPM capabilities.

The TPIV protocol works in the presence of an active adversary capable of adding memory to the node and ensures that a captured node does not reveal the secrets of other nodes. The performance improvement of the proposed TPIV protocol in terms of less computation, communication, and storage overhead is evident from the experimental results.

Goals and Assumptions

The goal of the TPIV protocol is to detect node capture attack that ensures the following.

1) Only an authorized verifier executes the PIV for detecting a node capture suspect.
2) A victim node cannot elude the PIV.
3) A captured node does not reveal the secret of other nodes.

The base station securely copies the free space contents of each node and one common copy of the remaining program memory content in each TVS. Using the initial platform configuration of TPM embedded in that TVS, the node program contents stored in a TVS are sealed.

For computation overhead, we only consider the time incurred in three main categories of operations, namely, public key, symmetric key, and heavy TPM operations such as TPM Unseal and TPM Sign, ignoring the lightweight operations such as XOR and TPM Read.

In the TPIV protocol, an awake node can immediately respond back to the server challenge, while in DAPP a node has to wait for the server to collect authentication tickets from other servers. In DAPP, anode as well as the verifying server has to compute polynomial based keys for all authentication tickets. Furthermore, to verify the authentication tickets, the MAC needs to be computed. In TPIV, a node performs only an unkeyed hash and three PRF operations.

References

[1]. P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Crypto*, 1999, pp. 388–397.

[2]. "Data encryption standard," Federal Inf. Process. Std. Publication 46,Nat. Bureau Std., Gaithersburg, MD, USA, Jan. 1977.

[3]. Advanced Encryption Standard (AES), *Federal Information Processing Standards Publication 197*, United States National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, 2002.

[4]. K. Okeya and T. Iwata, "Side channel attacks on message authentication codes," *Security Privacy Ad-hoc Sens. Netw.*, vol. 3813, pp. 478–488,2006.

[5]. S. Goldwasser and S.Micali, "Probabilistic encryption," *J. Comput. Syst.Sci.*, vol. 28, no. 2, pp. 270–299, Apr. 1984.

[6]. C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949

[7]. D. Dolev, D. Dwork, and M. Naor, "Non-malleable cryptography," *SIAM J. Comput.*, vol. 30, pp. 391–437, 2000.

[8]. A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1997.

[9]. A. Al-Hamadani and W. H. Allen, "RAAODV: A reputation-aware AODV for mobile ad hoc networks," in *Proc. ACM Southeast Regional Conf.*, 2014, Art. no. 6.

[10]. B. Wang, X. Chen, and W. Chang, "A light-weight trust-based QoSrouting algorithm for ad hoc networks," *Pervasive Mobile Comput.*,vol. 13, pp. 164–180, Aug. 2014.G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. 184–197, Mar./Apr. 2012.

[11]. S. Agrawal, M. L. Das, R. Roman, A. Mathuria, and J. Lopez, "A novel key update protocol in mobile sensor networks," in *Proc. 8th Int. Conf. Inf.Syst.Secur*,2012,vol.76

