Node Capture Attack in Wireless Sensor Network: A Survey

M. Vivekananda Bharathi[1], Rama Chaithanya Tanguturi[2], C. Jayakumar[3] and K. Selvamani[4]
[1]Student, R.M.K. Engineering College, Chennai, India
[2]Research Scholar, Department of Computer Science and Engineering, Anna University, Chennai, India
[3]Professor, Department of Computer Science and Engineering, R.M.K. Engineering College, Chennai, India
[4]Assistant Professor, Department of Computer Science and Engineering, Anna University, Chennai, India
([1]vibhacse@gmail.com, [2]trchaitanya@yahoo.com, [3]cjayakumar2007@gmail.com, [4]smani@cs.annauniv.edu)

Abstract - **Wireless Sensor Networks (WSNs) is an emerging and powerful technique for today's real world applications with interactive environments. The application of wireless sensor network starts from environment, household monitoring and ranging up to critical military applications. As their application involving in transmitting critical information, which require challenging methods to provide security for WSNs. Among various attacks in wireless sensor network, node capture attack is a serious attack through which an intruder can performs various operations on the network and can easily compromise the entire network. Node captures attack s one of the hazardous attack in WSNs. The wireless sensor network requires robust mechanism to improve the detection of node capture attack. Our survey analyzes various protocols and detection schemes to propose a new technique to achieve network resilience against node capture attacks.**

Keywords - **Wireless Sensor Networks, Security, Node Capture Attack**

I. INTRODUCTION

Wireless sensor network is a collection of large number of autonomous sensor node with low battery power, low memory storage and low cost devices. The transmission of sensitive information through sensor nodes requires strong security schemes. There are two levels of security mechanism namely low level and high level. The low level scheme includes security routing, resilience against node capture attack etc., and the high level includes intrusion detection, secure group management [1].

Key pre-distribution scheme is used for establishing a pair-wise key to obtain a secure communication between sensor nodes and also maintains network resilience against various attacks.

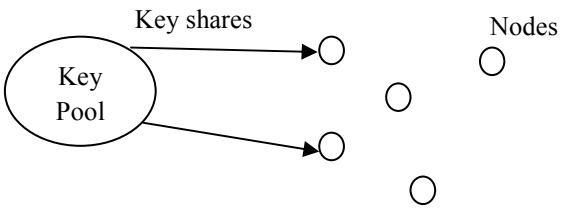

Fig.1. Key Pre-Distribution

Key Pre-distribution has three phases (i) Key distribution (ii) Shared key discovery (iii) Path key establishment. Each sensor nodes is allocated with a pool of keys before deploying into the sensor network as shown in fig.1. At the time of path establishment the nodes will exchange and compare their key IDs with the neighboring nodes. If there is a common key between the adjacent nodes then the pair-wise key is established between them. Polynomial based key distribution is used for the wireless sensor networks which will give resilience to the network even after a fraction of nodes in the network are captured till a threshold value is reached.

The Attacks are categorized into two types as active and passive attacks. Active attack includes routing attacks, eavesdropping etc., and passive attack includes all attacks against privacy [1]. Basically node capture attack remove sensor node for compromising from the network and redeploys them to perform various attacks. An adversary can modify the information, program and redeploys those malicious nodes in the network environment. The security mechanism needs to guarantee that, after the detection of node compromise till the revocation of the compromised nodes in the wireless sensor network, it should not affect the non compromised links. Securing wireless sensor network is becoming more critical when there are mobile nodes in the network. Mobility based attack detection is a challenging area in wireless sensor network security. As wireless sensor networks are resource constrained the security scheme should not introduce much complexity in term of identifying various attacks. This paper analyzes various schemes that are proposed to increase the resilience of the wireless sensor networks against node capture attacks.

II. RELATED WORKS

Generally Asymmetric key cryptosystem are not suitable for providing security in wireless sensor network because of their high computational requirements. The three new mechanisms proposed in [2] such as (i) Q-Composite keys scheme, (ii) Multipath- Reinforcement scheme and (iii) Random Pair wise keys scheme. Initially the sensor nodes are generated with key from key space before deploying into wireless sensor environment. These nodes cannot connect each other before establishing a common key. The shared secrete key leads to secure communication between sensor nodes. The existing Random key pre-distribution scheme performs the above task. In first scheme (Q-Composite), they estimated Q-common key

978-1-4673-1344-5/12/$31.00 ©2012 IEEE

Authorized licensed use limited to: b-on: Instituto Politecnico de Leiria. Downloaded on April 26,2022 at 17:27:03 UTC from IEEE Xplore. Restrictions apply.

for secure link between sensor nodes instead of single common key as key pre-distribution scheme. In second scheme (Multipath-Reinforcement) a new key is updated between two sensor nodes instead of using same common key that was installed prior to deployment. This would increase the network resilience against node capture attack. The communication between authorized sensor nodes is verified by node-to-node authentication. This is acquired through third scheme (Random Pair wise Keys Scheme). With these schemes we can achieve maximum resilience against node capture attacks as well as node replication.

Firdous Kausar et al. [3] proposed a new key pre-distribution scheme for pair-wise key setup in wireless sensor network. Each sensor node is allocated with small number of random key before deployment. After deployment, each node passes their key and node ID to their neighbor nodes for sharing pair-wise keys. These shared pair-wise key is generated independently through keyed hash algorithm over generated keys in node. The initial key ring is deleted from node memory and new key is generated through pseudo random function to allow node to join the network. Thus, the scheme provides more resilience against node capture and reduces the node memory by deleting initial key ring.

Whereas, the scheme proposed scheme by [4] quickly detects captured node using Sequential Probability Ratio Test (SPRT). The absence of captured node is identified using pre-defined threshold value. The time period of the missing node is more than the threshold value indicates that sensor node is captured. This scheme detects the node capture attack efficiently and also limits the time duration of captured node within five time slots to prevent them from being detected.

A framework proposed [5] for node capture attack which includes physical node capture, cloned node detection and revocation of compromised nodes. A dynamical model is used to describe the behavior of node in the network under attack. It is derived by combining both probabilistic analysis of logical key graphs and linear control theory. The Linear Quadratic Regulator (LQR) and Linear Quadratic Gaussian (LQG) methods are derived to control the network response to node capture attacks and to revoke the compromised node from the wireless sensor network. The computation of optimal revocation rates acquire secured network connectivity under attack. So provides resilience against physical node capture attack.

A symmetric matrices of key is used for generating single secrete key for establishing a secure communication whereas Modified Bloom's Scheme (MBS) [6] uses Asymmetric matrices of key to generate pair-wise key between two sensor nodes. The sensor node carries master secret key in a tamper resistant hardware will increase the cost and energy consumption of each node. They generate two secret keys to communicate between sensor nodes. Asymmetric Matrices provides bidirectional link between pairs of nodes. This scheme decreases compromised communication link between two nodes in the network. The network resilience against node capture attack is improved by increasing the number of keys generated in each sensor nodes. Base station analyzes the replication of node through the list of neighbor's location through centralized detection scheme and centralized mechanisms do not detect distributed replication efficiently. Two algorithms in [7] described such as Randomized Multicast Protocol to distribute node information and Line-Selected Multicast uses the topology of network to detect replication. Nodes in wireless sensor network act as both sensing unit as well as routers. The Randomized Multicast Protocol prevents adversary through identity of the witness and has same communication overhead as that of broadcast scheme. The Line Selected Multicast reduces the communication overhead of randomized multicast protocol through intermediate nodes. Thus provides excellent resilience against replication of node in the network.

The two protocols proposed by Mauro Conti et al. [8] is Simple Distributed Detection (SDD) and Cooperative Distributed Detection (CDD) to detect the node capture attack in a mobile wireless sensor network. Each node in wireless sensor network feels the presence of their neighbor nodes through False Alarm Neutralization (FAN) mechanism. If node (say A) does not replying to node (say B) within the estimated time indicates the absence of node (A) in the network. The attackers remove the node before capturing and it is detected using the local information of the nodes. The Cooperative Distributed Detection protocol collaborate the node to improve the detection of node capture attack in the network.

Providing security is a challenging issue in wireless sensor network. The sensor nodes communicate securely through key pre-distribution schemes. Two key pre-distribution [9] schemes are proposed and the first scheme is obtained by combination of Polynomial Pool based Key Pre-distribution and probabilistic generation key pre-distribution. A key is generated from pool of random bi-variate polynomial and random generation key with unique ID. Sensor node can communicate by establishing pair-wise key. Node (A) can directly communicate to node (B) or indirectly communicate through intermediate node (I). The second scheme is obtained by combining Q-Composite Generation with Polynomial Pool based Scheme which increase the number of generation key instead of single common key. This will reduce the size of the pool and improves the resilience of the network against node capture attack. The proposed scheme will reduce the percentage of compromised sensor node below 45-29 percent.

This paper summarizes various existing techniques and methodologies to prevent such type of attacks in WSNs. Some of them are listed in Table I and Table II.

Table I and Table II shows the summarized existing mechanisms that provides resilience against nod capture attack. Table I indicates the schemes that uses key establishment methods for securing the wireless sensor

Authorized licensed use limited to: b-on: Instituto Politecnico de Leiria. Downloaded on April 26,2022 at 17:27:03 UTC from IEEE Xplore. Restrictions apply.

network. Table II describes the various works which are used to detect the node capture attacks.

TABLE I
METHODS BASED ON THE KEY ESTABLISHMENT

Reference	Key Establishment Methods	Distributed Scheme	Mobility Support
[2]	(i)Q-Composite Scheme. (ii)Multipath Reinforcement Scheme. (iii)Random Pair wise keys Scheme.	No	No
[3]	Pair wise key Pre-distribution Scheme	Yes	No
[6]	Asymmetric Matrices Key Pre-distribution	No	No
[9]	(i)Combines Polynomial Pool-Based Key Pre-Distribution and Probabilistic Generation Key Pre-Distribution. (ii)Combines Q-Composite generation with Polynomial Pool-Based Scheme.	No	Yes (Only for mobile sink)

TABLE II
METHODS TO SECURE AGAINST NODE CAPTURE ATTACK WITHOUT KEY

Reference	Proposed Methods	Distributed Schemes	Mobility Support
[4]	Sequenced Probability Radio Test (SPRT)	Yes	No
[5]	Linear Quadratic Regular (LQR)and Linear Quadratic Gaussian (LQG) Method	No	No
[7]	(i)Randomized Multicast Protocol. (ii)Line-Selected Multicast.	Yes	No
[8]	(i)Simple Distributed Detection (SDD). (ii)Cooperative Distributed Detection (CDD).	No	Yes

III. CONCLUSION

We discussed various security schemes for node capture attack in detail. These mechanisms require time to notice some activities on the network to detect the node capture. Most of the existing schemes are not detecting the node capture attack immediately. More research is needed to have an immediate detection mechanism towards node capture attack in wireless sensor network.

IV. FUTURE WORK

Our future work is to build a frame work which gives immediate resilience against various attacks like node capture attack in wireless sensor network.

REFERENCES

[1] V. J. Rathod, M. Mehta, "Security in Wireless Sensor Network:A Survey", Ganpat Univ. J Eng Technology, vol. 1, no. 1, pp. 35-44, 2011.

[2] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks", in *Proc. IEEE Sym. Security and Privacy*, pp. 197, 2003.

[3] Firdous Kausar, Sajid Hussain, Tai-hoon Kim, and Ashraf Masood, "Attack Resilient Random Key Distribution Scheme for Distributed Sensor Networks", Emerging Direction in Embedded and Ubiquitous Computing Lecture Notes in Computer Science, vol. 4809, pp. 1–11, 2007.

[4] Jun-Won Ho, "Distributed Detection of Node Capture Attacks in Wireless Sensor Networks", in *Smart Wireless Sensor Networks*, pp. 345-360, 2010.

[5] T. Bonaci, L. Bushnell, R. Poovendran, "Node Capture Attacks in Wireless Sensor Networks:A System Theoretic Approach", IEEE *Conf. on Decision and Control (CDC)*, pp. 6765 – 6772, 2010.

[6] K. Shaila, S. H. Manjula, J. Thriveni, K. R. Venugopal, and L. M. Patnaik, " Resilience Against Node Capture Attack using Asymmetric Matrices in Key Predistribution Scheme in Wireless Sensor Networks", International Journal on Computer Science and Engineering, vol. 3, pp. 3490-3501, 2011.

[7] Bryan Parno , Adrian Perrig , Virgil Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks", IEEE Symposium on Security and Privacy, p.49-63, 2005.

[8] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei, "Emergent Properties: Detection of the Node-capture Attack in Mobile Wireless Sensor Networks," in Proc. 1st Conf.Wireless Network Security, pp. 214-219, 2008.

[9] Amar Rasheed and Rabi N. Mahapatra, "Key Pre-distribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks", *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 1, pp. 176-184, 2011.

Authorized licensed use limited to: b-on: Instituto Politecnico de Leiria. Downloaded on April 26,2022 at 17:27:03 UTC from IEEE Xplore. Restrictions apply.