I.J. Computer Network and Information Security, **2014, 11, 26-34**
Published Online October 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.11.04

Optimized and Executive Survey of Physical Node Capture Attack in Wireless Sensor Network

Bhavana Butani
University Institute of Technology, RGPV, Bhopal, 462036, India
Email: bhavanabutani89@gmail.com

Dr. Piyush Kumar Shukla and Dr. Sanjay Silakari
University Institute of Technology, RGPV, Bhopal, 462036, India
Email: pphdwss@gmail.com, ssilakari@yahoo.com

***Abstract*—**Wireless sensor networks (WSNs) are novel large-scale wireless networks that consist of distributed, self organizing, low-power, low-cost, tiny sensor devices to cooperatively collect information through infrastructure less wireless networks. These networks are envisioned to play a crucial role in variety of applications like critical military surveillance applications, forest fire monitoring, commercial applications such as building security monitoring, traffic surveillance, habitat monitoring and smart homes and many more scenarios. Node capture attack is one of the most dreadful security attack exist in wireless sensor networks. An adversary steals cryptographic key or other confidential information like node's id etc from a captured node to compromise entire network. So, Security of wireless sensor network is an important issue for maintaining confidentiality and integrity of wireless links. Now-a-days, researchers are paying attention towards developing security schemes against Node capture attack. Our survey provides deep insights of existing techniques that enhance the attacking efficiency of the node capture attack in wireless sensor network. It also analyzes various detection and key pre-distribution schemes for inventing a new scheme to improve resilience against node capture attack.

***Index Terms*—**Wireless Sensor Network, Node Capture Attack, security, Key pre-distributions, VANET.

I. INTRODUCTION

Wireless Sensor Networks are heterogeneous systems containing several tiny devices known as sensor nodes and actuators with general computing components. These networks will composed of lots of low cost, low power and self-organizing sensor nodes which are distributed either within the network or near it. These sensor nodes contain three main elements-sensing, data processing and communication. Two other elements are also there called, aggregation and base station. Aggregation nodes collects data from the nodes located near it combines the collected data and then sends it to the base station. Figure 1 illustrates the basic architecture of wireless sensor network. The Numerous applications of Wireless sensor network includes habitat monitoring, manufacturing and logistics, environmental observation and forecast systems, military applications, health, home and office application and a variety of intelligent and smart systems. The computation and processing ability of sensing nodes

are limited as a result of nodes affected by energy constraint because they are run by battery power. Robust security schemes are needed for transmitting secured information using sensor nodes within the network. There exist two levels of security schemes, low level and high level. The low level scheme includes secured routing, resilience against node capture attack, privacy, Key establishment and trust setup etc., and High level scheme includes intrusion detection, secure group management and secure data aggregation.

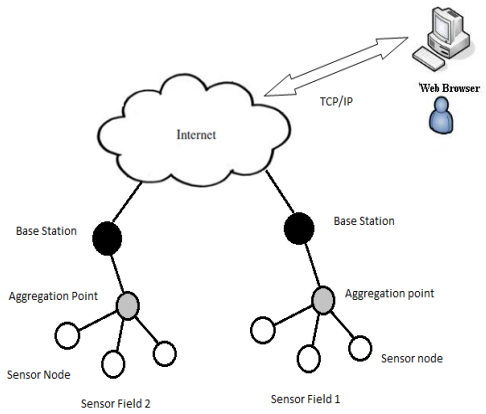

Fig. 1. Wireless Sensor Network Overview

The Attacks are mainly divided into two types as active and passive attacks. In Active attack, the unauthorized attacker's monitors, listen to and modifies the data stream in the packet exchange within the network. Active attack includes routing attacks, eavesdropping and creation of a false stream etc. The monitoring and eavesdropping on the packet exchange by unauthorized attackers within a WSN are known as passive attack. Passive attack includes all attacks against privacy like monitor and eavesdropping, traffic analysis, camouflage adversaries. Basically node capture attack captures a particular node within the network. Then removes that compromised node from the network and redeploys them for performing diverse attacks. An adversary can alter the

information, program and redeploys those malicious nodes within the network environment. The security mechanism goes to have to guarantee that, when the compromised nodes are detected into the WSN, the non-compromised links should not be affected until the redeployment of the compromised nodes in the WSN. Security of a sensor network is more important when there exist mobile nodes in the network.

The rest of this paper is structured as follows. In Section II, we mention the description of the node capture attack. In Section III, we provide a survey of modeling of node capture attacks using different techniques. Section IV includes various protocols and detection schemes used for network resilience against node capture attacks. Section V includes conclusion.

II. Node capture attack

Node capture attack is the combination of passive, active, and physical attack by an intelligent adversary. In WSN, security is important to preserve confidentiality and integrity of the wireless links. These two properties of network can be lost by physically capturing nodes and stealing important information from their memories like cryptographic keys, its unique id, information to communicate within the network etc. This type of attack is called the node capture attack in which an external adversary can capture a sensor node to get access to the cryptographic keys to break the security of link layer mechanism. By recovering the essential information from the nodes memories, an attacker can eavesdrop communication within the network. This type of attack largely destroys the security, integrity and confidentiality of the network. Once the attacker captures a set of sensor nodes, these nodes can be altered in terms of both software programming and hardware configuration. This access of an adversary by capturing a set of sensor nodes can then be used to launch further attacks on the network.

III. Survey Of Modeling Of Node Capture Attack Using Different Schemes

Tague et al. presented a mathematical model for node capture attacks on key establishment protocols in heterogeneous wireless ad hoc and mesh networks. This mathematical model relates the information brought by an attacker to the sets Sn assigned to nodes in N. By defining the amortized initialization overhead cost as well as the cost of capturing each node and the contribution of each node to the attack success, node capture attacks are formulated using an integer programming minimization problem. They identified problem that there is no polynomial solution that can determine the node capture attack with minimum cost for heterogeneous or homogeneous networks. An efficient heuristic algorithm for node capture attacks was thus presented using a known heuristic for the integer-programming minimization problem. They shown that, by the use of privacy- preserving key establishment protocol, the attack can be prevented using a subset coverage strategy. They also investigated storage randomization as a technique to mitigate set coverage attacks. They also shown, even in the presence of storage randomization, the adversary can perform a probabilistic heuristic via statistical analysis at an increased cost. They observed that the probabilistic heuristic outperforms the random capture of nodes [1].

Tague et al. [2] also formalized a model for node capture attack in which an attacker collects information about the network by eavesdropping on the wireless medium and captures nodes based on the learned information. Use of open, shared wireless medium allows any nearby device to overhear message transmission, interference with or block message reception, insert messages within the network. Even if the message payload is encrypted, the exchange of messages and the presence of message headers potentially allow an eavesdropper to learn about the network operation and the protocol state. In addition to passive learning, the attacker can actively participate in network protocols, probing the network for information and maliciously injecting the information into the network. Once sufficient amount of information is achieved by the adversary, he can physically capture nodes. The gathered information is used by the adversary in order to optimize the performance of the attack. The author showed that the goal of node capture attack can be decomposed into a collection of primitive events, the influence of which can be estimated and recollected to yield an overall of the attack. They considered the attack correspond to NP-hard optimization problems and discussed the behavior of a reasonable heuristic algorithm. They used the event based attack decomposition model for the development of suitable performance metrics for node capture attack. They also discussed the potential use of event based decomposition and evaluation metrics for the purpose of defend against node capture attack.

Tague et al. also given that when security and routing protocols are analyzed independently, the vulnerabilities of secure network traffic remain undetected. In this work [3], the authors took into consideration joint analysis of security and routing protocols in wireless networks to reveal vulnerabilities. The authors investigate a class of continuous metrics to evaluate the vulnerability of network traffic and isolate weakly secured connections. They devised two complementary vulnerability definitions by using set theoretic and circuit theoretic interpretations. These definitions of vulnerability allow an adversary to determine weakness or vulnerable point in the secure network. They also formulated the node capture attack as a nonlinear integer programming minimization problem. Due to the NP hardness of minimization problem, they presented the GNAVE algorithm, a Greedy Node Capture Approximation using Vulnerability Evaluation using a greedy heuristic to approximate the minimum cost attack. The use of greedy heuristics allows it to iteratively add nodes to the set of compromised nodes to maximize the increase in route vulnerability at each step. To increase the route vulnerability with minimum resource expenditure, it is

beneficial for an attacker to attempt to increase the vulnerability which results from the capture of each individual node through the information recovered from previously captured nodes. To enhance the cost effectiveness of the node capture attack at each step, an attacker chooses to compromise the node with maximum incremental value per unit cost. GNAVE can enhance attacking efficiency in terms of fewer compromised nodes and higher fraction of compromised traffic, but it did not include the execution time to compromise the network.

De et al. proposed in [4] proposed the spreading process of node compromise in large-scale sensor networks. To study the results and effects of node capture attack, the author expressed the spread process to compromise the node by using epidemic theory. They started from a single most vulnerable point, and then assumed that the neighboring nodes can be compromised by an adversary via wireless communication and thus can threaten the complete network. As a result of security schemes used by the sensor networks, they assumed that communication can only be established when neighboring nodes can establish mutual trust by sharing a common key. Therefore, they shown that node compromise is not solely determined by the deployment of sensor nodes that successively affects node density, but also determined by the pair wise key scheme used in that. By taking these factors of the networks, they proposed an epidemiological model to identify the probability of a breakout (compromise of the whole network) and if not, the sizes of the components that are affected. Moreover, they analyzed the result of node recovery in an active infection state of the network and got vital values for these parameters that resulted in an outbreak. They targeted their analysis on two specific kinds of node deployment scenarios, namely uniform random deployment and group based deployment of nodes. Their results showed that a uniform random deployment was more insecure to epidemic propagation than a group-based deployment model and leak key parameters of the network in defensive and containing potential epidemics. In the case of the node recovery, the result provided benchmark time period for the network to recover a node so as to defend against the epidemic spreading and also vital values of the key sharing probability which characterize the transition from a non epidemic to an outbreak state of the network compromise. However, the authors neglected to think about that an attacker can capture more than one node within the network to compromise the network. Therefore, modeling process of the node capture attack as a spread process is not suitable.

Bonaci et al. proposed a control-theoretic framework to model physical node capture attacks in WSN by mapping the network security problem into a control theory problem. They also taken detection of cloned nodes and recovery of compromised node, followed by key distribution to valid nodes into consideration. By using probabilistic analysis of logical key graphs with linear control theory, they proposed a dynamical model that efficiently describes network behavior under attack. Using control theory methods, they showed that the network response under node capture attacks can be characterized using a proportional controller. They devised two network response strategies based on optimal control theory and showed the optimization problem can be formulated explicitly in terms of the network as well as logical key graph parameters. Using optimal control theory, they obtained the minimal revocation rate as a control parameter, which guarantees secure network connectivity and hence stability under the attack. The practical implications of these are: it enables (a) analysis of the network's stability and resilience against the physical node capture attack, (b) characterization of adversarial behavior and strategies and (c) computation of the optimal revocation rates, in terms of network parameters and cryptographic quantities, to maintain secure network connectivity in the presence of the attack. In this model, the authors provide consideration for the behavior of the attacker, while the effects of the node capture attack are not fully considered [5].

Mishra et al. proposed probabilistic model to capture a node in WSN by an adversary. An Adversary physically captures a node to steal all the secure information which is stored into the node's memory to lunch further attacks by deploying clones of a compromised node. To achieve this goal, an adversary needs to gather information for the network to capture a node. So they identified, to capture a node it is necessary for an adversary how quickly he/she is able to gather information regarding the network and for the target node. In this work, they modeled the information gathering process by an adversary to capture a node as a birth and death process. They shown that the time varies to gather information for different attackers based on their strength and configuration. So they also proposed the expected time of node capture based on the strength of an adversary and dynamicity of the network using a stochastic process. They also calculated expected amount of information that will be available to an adversary at an arbitrary time t [6].

In this paper [7], a high efficiency node capture attack algorithm based on route minimum key set, namely GNRMK, is presented. In GNRMK, the wireless sensor network is mapped as a flow network and therefore the link key set cardinal is formalized as the capacity of the corresponding edge in flow network to get its route minimum key set that shows the vulnerability of the route in the network. The route minimum key set can be achieved by computing the max flow of the flow network using labeling and adjustment procedure on the basis of Ford– Fulkerson. In the label procedure, an augment path is found using breadth-first search. Then, they have the adjustment value, which can be found within the last searched node. In the adjustment procedure, if the edge is pointing toward the destination node, the flow value of each edge on the augment path is updated by adding the adjustment value in it otherwise subtracting the adjustment value if the edge is pointing toward the source node. The max flow is estimated through finding augment paths regularly. Then, a node overlapping value (NOV) metric is estimated through the route minimum key sets.

A node with maximum overlapping value is targeted as the node to be compromised. Also, when a node is compromised, the topology of the network is dynamically modified because of the already compromised links or paths. So, the algorithm needs to traverse all the paths within the sensor network and delete the compromised paths because of the compromised key set estimated by captured node set. In this way, a new sensor network topology is acquired with the paths that are not compromised yet. Every time the network is restructured just after a node compromised and in this way, the complexity of the network is quickly reduced. Thus, the attack times out, and executing time may be reduced effectively. The effect of GNRMK algorithm is shown in different routing environments: the single path routing protocol, the multiple independent path routing protocol, and the multiple dependent path routing protocol. Furthermore, GNRMK is compared with previously related proposed schemes that show that GNRMK provides more efficiency in compromising the network.

Chi Lin et al. approached the node capture attack from an attacker's point of view and developed a matrix approach to design the process of node capture attack. The authors proposed Matrix Algorithm (MA) which can produce the maximum destructiveness while taking the minimum resource expenditure (Energy cost). They established a matrix to show the compromising relationship among nodes and the paths [8]. To indicate the compromise relationship, first they analyzed the relationship between the paths and key by establishing path-key matrix PK = [pki, j] P ×K that clears that whether obtaining a single key can directly lead to compromise of a path. Then they created another key-node matrix KN = [kni, j] K ×N for showing the belonging relationship between the keys and the nodes. After that, they derived compromise relationship between nodes and paths by establishing the matrix PN = [pni, j] P ×N as PN = PK ×KN. But it may be possible that a link is secured using more than one key. So considering only direct compromise relationship is not enough. To show partial compromise relationship they established another matrix PLN = [plni, j] P ×N for representing the ratio of keys which are acquired by the adversary in path pi when node nj is captured. Then they combine the entries of PN and PLN into another matrix M = [mi, j] P ×N to represent compromise relationship. The adversary looks for compromising a set of nodes that can compromise the entire network while taking the least energy. Thus, the author combines energy cost of capturing nodes into the matrix MC = [mci, j] P ×N. After that, they devised the node capture attack algorithm to enhance the attacking efficiency. They performed the lots of experiments to check the performance of MA. Results show that MA reduced the attacking rounds, shorten the execution time, enhancing the attacking efficiency and conserve the energy cost. They modeled the MA algorithm that is limited to random key pre-distribution scheme. It also paid little attention to the relationship between the attacking efficiency and the attacking cost [8].

Design an efficient node capture attack algorithm is challenging for dynamic network topology. In this paper [9], the author proposed a general algorithm to model node compromise attack in VANET. In their method, they defined the destructiveness value SK (i) to show the number of vehicles which are sharing keys with node i. These algorithms enhance the attacking efficiency by destroying the network backbone. The Connected Dominating Set of the network is used to construct the backbone. In VANET, nodes are moving over time so creation of fixed backbone is impossible task. To overcome this difficulty, they construct the virtual backbone. They construct Connected Dominating Set (CDS) as virtual backbone for balancing load and maintaining connectivity using dominating Set. The author proposed two attacking algorithm based on the general model to destroy the network in the centralized and distributed network while maximize the destructiveness. In Centralized attack based on Connected Dominating Set (CCDS), when adversary finds the target node to attack, he calculates the value of SK () for the neighbor nodes of all the captured nodes. Then he finds the node with the maximum value to mount an attack which will cause the maximum destructiveness within the network. In distributed attack based on Connected Dominating Set (DCDS), an adversary can select any node in CDS to attack. In the DCDS, an adversary needs to find the attacking node in each iteration. An adversary initially records the key sharing relationship and computes the value of SK (). Then he finds the vehicle with the maximum SK () and provides the index of the vehicle as the output. They compare DCDS and CCDS with two node compromise attack algorithms: random attack and epidemic attack. Simulation results show that their scheme improves the attacking efficiency in different mobility models and different applications. Regardless of specific key distribution scheme, in their work, the probability that two neighboring nodes share at least one key to establish a secure communication is represented by α. So, when they developed general model to formulize the node compromise attack, there was no need to consider what key pre-distribution protocol was implemented. They only focused on the influence of α to the attacking efficiency.

Table 1 represents existing approaches for modeling of node capture attack in the wireless sensor network.

IV. Survey Of Various Detection And Key Predistribution Schemes Used For Resilience Against Node Capture Attack

Generally Asymmetric key cryptosystem don't seem to be appropriate for maintaining security in wireless sensor network as a result of their large computational requirements. The three new mechanisms proposed in [10] such as (i) Q-Composite keys scheme. (ii) Multipath-Reinforcement scheme and (iii) Random Pair wise keys scheme. Initially the sensor nodes are assigned some keys

from the key pool before deploying it into a wireless sensor network. These nodes cannot communicate with each other before sharing the same secret key. The shared secret key provides secure communication between sensor nodes. Above task is performed by the existing Random key pre-distribution scheme. In the first scheme

Table 1. Different Approaches for modeling of Node Capture Attack in WSN

Authors	**Tague et al[1]**	**Tague et al[2]**	**Tague et al.[3]**	**De P et al. [4]**	**Bonaci et al.[5]**	**Mishra et al.[6]**	**Wu G et al.[7]**	**Chi Lin et al. [8]**	**Chi Lin et al. [9]**
Proposed Works	Modeling of Node Capture Attacks using Different Greedy heuristics in multi-hop wireless networks.	Modeling of Node Capture Attacks as an NP- hard optimization problem in Wireless sensor Network.	Modeling of Node Capture Attacks using GNAVE algorithm.	Modeling of Node Compromise that captures the unique topological characteristics of deployed wireless sensor network using pairwise key schemes.	Study of Physical Node Capture using a Control Theory Framework.	Model of information gathering process by an attacker For Node Capture Attack.	Modeling of node capture attack algorithm based on route minimum key set (GNRMK).	Modeling of Node Capture attack algorithm using a matrix approach.	Two attacking algorithms (CCDS and DCDS) are modeled based on the proposed general algorithm for centralized and Distributed Version of attack.
Approach	Vulnerability evaluation approach	Vulnerability evaluation approach	Vulnerability evaluation approach	Epidemic Theory	Probabilistic analysis (System theoretic model)	Probabilistic analysis	Vulnerability evaluation approach	Vulnerability evaluation approach	Vulnerability evaluation approach
Centralized/ Distributed Attack	Distributed Attack	Distributed Attack	Distributed Attack	Centralized Attack	Distributed Attack	Distributed Attack	Distributed Attack	Distributed Attack	Centralized and Distributed Attack
Limitations	Modeling of Node Capture Attack is presented only for probabilistic and Deterministic Key distribution schemes. It is only theoretical concept. It is not implemented practically.	Modeling of node capture attack focused only on the relationship between nodes and routes. This results in a long execution time.	GNAVE does not consider execution time while mounting the node capture attack for compromising the network	De et al. studied the epidemic propagation method which focused on the effect of different network deployment, however neglected the mobility of the nodes within the network. It also neglects that an attacker can capture more than one node within the network while mounting an attack.	Overestimated the issue of attacking efficiency and resource expenditure in mounting an attack. It only focuses on the behavior of the attacker, while the results of attack are not completely considered.	Difficult to find how much amount of information is gathered by an attacker to compromise the network	GNRMK can only be utilized in the static network with deterministic key distribution protocol that is not appropriate for VANET.	MA paid little attention to relationship between attacking efficiency and attacking cost. It is also restricted for random key predistribution protocol.	It is suitable for some nodal mobility models like CMC, RWP.
Random/ Dynamic Node Capture	Dynamic	Dynamic	Dynamic	Random	Random	Random	Dynamic	Dynamic	Dynamic

To figure axis labels, use words rather than symbols. Do not label axes only with units. Do not label axes with a ratio of quantities and units. Figure labels should be legible, about 9-point type.

Color figures will be appearing only in online publication. All figures will be black and white graphs in print publication.

(Q-Composite), Q-common secret keys are needed instead of a single common sharing key as a key pre-distribution scheme to secure the link between sensor nodes. In the second scheme (Multipath-Reinforcement), a new secret key is assigned between two sensor nodes rather than using the same secret key that was allocated prior to deployment. This would enhance the network resilience against node capture attack. Node-to-node authentication scheme is used to verify communication between legitimate sensor nodes. This is achieved using third scheme (Random Pair wise Keys Scheme). With these schemes, we can obtain improved resilience against node capture attacks as well as node replication.

The scheme presented by [11] quickly observes compromised node through Sequential Probability Ratio Test (SPRT). The absence of captured node is found out through pre-defined threshold limit. When threshold limit is less than the time period of the missing node, this condition indicates that the sensor node is captured. This scheme detects the node capture attack with more efficiency and additionally limits the time period of a captured node inside five time slots to prevent them from being detected.

A framework presented [5] for node capture attack which has physical node capture, cloned node detection and revocation of compromised nodes. A dynamical model is employed to explain the behavior of a node within the network under node capture attack. This model is conceived by taking both probabilistic analysis of logical key graphs and linear control theory into account. The Linear Quadratic Regulator (LQR) and Linear Quadratic Gaussian (LQG) methods are intended to control the response of the network under node capture attacks and to revoke the captured node from the wireless sensor network. The estimation of optimal revocation rates gain secured network connectivity under attack. Thus provides resilience against node capture attack.

Symmetric matrices of key is utilized for generating a shared secret key to establish a secure communication whereas Asymmetric matrices of key is utilized by Modified Bloom's Scheme (MBS) [12] for generating pair-wise key between two sensor nodes. Each sensor node stores master secret key in a tamper resistant hardware that will enhance the cost and energy consumption of the node. They established two shared secret keys to provide communication between sensor nodes. Bidirectional link is made available by the Asymmetric Matrices between pairs of nodes. This method reduces communication link that is compromised between two nodes within the network. Network resilience against node capture attack is enhanced by enhancing the amount of keys generated in each sensor nodes. Base station examines the node replication through the list of neighbor's location using centralized detection scheme and centralized mechanisms does not analyze distributed replication effectively. Two algorithms in [13] proposed such as Randomized Multicast Protocol to distribute node information and Line-Selected multicast uses the topology of the network to find replication. Nodes in wireless sensor network work like sensing unit as well as routers. An adversary is prevented by Randomized Multicast Protocol using witness identity. It has same communication overhead as that of broadcast scheme. The Line Selected Multicast uses intermediate nodes to reduce the communication overhead of randomized multicast protocol. So provides improved resilience against replication of the node within the network.

The sensor nodes establish secure communication using key pre-distribution schemes in the WSN. In this paper [14], the author proposed two key pre-distribution schemes. The first scheme is acquired by a combination of Polynomial Pool based Key Pre-distribution and probabilistic generation key pre-distribution. A secured key is generated from a pool of random bi-variate polynomial and random generation key with a unique ID. Sensor node can establish a communication by establishing secured pair-wise key. Node (A) can directly or indirectly communicate to node (B) using an intermediate node (I). The second scheme is acquired by using Q-Composite key generation with Polynomial Pool based scheme that enhance the number of generation key rather than a single common key. This will minimize the size of the key pool and provides better resilience against node capture attack in the network. The proposed scheme will minimize the percentage of captured sensor node below 45-29 percent.

In this paper [15], the author presented the ICmetric technique to provide safeguard against node capture attack in WSN. ICmetrics or Integrated Circuit metric generates shared keys for secure communication by making use of hardware and software characteristics. It is very hard for an adversary to deduce these characteristics. This metric or feature is not static, but in a pre-determined manner. It is not dependent on any particular encryption algorithm. It generates an encryption key from measurable properties of any hardware and software properties of the sensor node. When an attacker tampers with hardware and software properties of the sensor node, it will change its parameters that will result in different computed ICmetric. This change will reflect an indication that the sensor node has been tampered. Therefore, the use of ICmetric improves resilience against node capture attack.

In this paper [16], the authors provides a network model appropriate for their proposed key management scheme supporting mobility in a heterogeneous WSN that consists of mobile sensor nodes with some static sensor nodes. This scheme based on the two disjoint key pools through which communication keys and authentication keys are derived. These two disjoint key pools gives better security by taking less memory space. They also showed that when a mobile node is in the radio coverage

range of more than one static node and this result strongly support for node mobility in WSN then network connectivity in terms of authentication key sharing probability enhances. This scheme also provides improved network resilience against node capture attack compared to some basic schemes.

Table 2. Mechanisms to secure network against node capture attack

Authors	H. Chan et al.[10]	Jun-Won Ho[11]	Bonaci et al.[5]	K. Shaila et al.[12]	Bryan Parno et al.[13]	Amar Rasheed et al.[14]	Ruhma Tahir et al.[15]	Sarmad Ullah et al. [16]	T.D.Subash et al.[17]	S.H. Jokhio et al.[18]
Proposed Works	(i)Q-Composite Scheme. (ii)Multipath Reinforcement Scheme. (iii)Random Pair wise keys Scheme.	Sequenced Probability Radio Test (SPRT)	Linear Quadratic Regular (LQR)and Linear Quadratic Gaussian (LQG) Method	Asymmetric Matrices Key Predistribution	i)Randomized Multicast Protocol. (ii)Line-Selected Multicast.	(i)Combines Polynomial Pool-Based Key Pre-Distribution and Probabilistic Generation Key Pre-Distribution. (ii)Combines Q-Composite generation with Polynomial Pool-Based Scheme.	ICmetric Scheme	A Key Management Scheme Supporting Node Mobility in Heterogeneous Sensor Network	Hashed key management scheme	Sensor node capture attack detection and Defense(SCADD) protocol
Distributed Schemes	No	Yes	No	No	Yes	No	Yes	Yes	Yes	No
Mobility Support	No	No	No	No	No	Yes (only for mobile sink)	No	Yes	No	No
Based on Key Establishment	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No

In this paper [17], the authors proposed Hashed key management scheme and deployment model for WSN. These scheme uses hash function to prevent adversary to get information about non- compromised sensor nodes from the compromised sensor nodes and the deployment model which is based on hexagonal for enhancing the local connectivity within the network. The main advantage of these scheme is that an adversary cannot gather key information after pair-wise key establishment, because it is computationally infeasible to revert the hash function. So, this scheme provides the best resilience against nodes capture attack.

The authors proposed [18] the SCADD protocol for node capture attack detection and defense in WSN. SCADD gives a cost-effective solution against the node capture attacks in WSNs, increases the security of WSN for security-sensitive applications. SCADD consists of two building blocks: node attack detection and defense advocating measure block. The node attack detection block provides strategic-based attack detection to abolish the possibility of misjudgment and other block uses a self-destruction defense measure against node capture attack to avoid significant security while not really destroying the node's radio service.

Table 2 represents the summarized existing mechanisms that provide resilience against node capture attack.

V. Conclusions

In this paper, we studied different modeling techniques of node capture attack using different approaches like Vulnerability evaluation approach, Epidemic Theory, Probability analysis etc. We also provided the characterization of these modeling techniques into centralized and distributed version of attack. In centralized version of attack, an attacker can start from single most vulnerable node and then assumed that the neighboring nodes can be compromised via wireless links

and thus can threaten the entire network. In distributed attack, an adversary can select random node to capture. Table provides information about different modeling technique of node capture attack with their respective limitations. We also mentioned various detection and key pre-distribution schemes that provide resilience against node capture attack. Researching the mechanism of node capture attack provides deep insights to design robust defending and detection mechanism to improve resilience against node capture attack in WSN.

REFERENCES

[1] Tague P, Poovendran R, "Modeling adaptive node capture attacks in multi-hop wireless networks", In Ad Hoc Network, Vol. 5, No. 6, pp. 801–814, 2007.

[2] Tague P, Poovendran R, "Modeling node capture attacks in wireless sensor networks", In: Proc 46th annual Allerton conference on communication, control, and computing, pp 1221–1224, 2008.

[3] Tague P, Slater D, Rogers J, Poovendran R, "Evaluating the vulnerability of network traffic using joint security and routing analysis", IEEE Trans Dependable Secure Comput, Vol. 6,No. 2, pp. 111–123, 2008.

[4] De P, Liu Y, Das S, "Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory", In ACM Trans Sensor Network, Vol. 5, No. 3, pp. 1–33, 2009.

[5] Bonaci T, Bushnell L, Poovendran R, "Node capture attacks in wireless sensor networks: a system theoretic approach", In: Proc IEEE 49th international conference on decision and control, pp. 6765–6772, 2010.

[6] Mishra A, Turuk A, "Adversary information gathering model for node capture attack in wireless sensor networks", In: Proc IEEE international conference in devices and communication, pp. 1–5, 2010.

[7] Wu G, Chen X, Obaidat MS, Lin C, "A high efficient node capture attack algorithm in wireless sensor network based on route minimum key set", In Secure Communication Network, 2012.

[8] Chi Lin, GW, Enhancing the attacking efficiency of the node capture attack in wsn: a matrix approach, J Supercomput, 2013.

[9] Chi Lin, Guowei Wu, Feng Xia, Lin Yao, "Enhancing Efficiency of Node Compromise Attacks in Vehicular Ad-hoc Networks Using Connected Dominating Set", In Mobile Networks and Applications, Vol. 18, No. 6, pp. 908-922, 2013.

[10] H. Chan, A. Perrig, and D. Song, "Random Key Pre-distribution Schemes for Sensor Networks", In Proc. IEEE Sym. Security and Privacy, pp. 197, 2003.

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

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

[13] Bryan Parno, Adrian Perrig, and Virgil Gligor, "Distributed detection of node replication attacks in sensor networks", In Proceedings of the IEEE Symposium on Security and Privacy, pages 49–63, May 2005.

[14] 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.

[15] Ruhma Tahir, Klaus McDonald-Maier, "Improving resilience against Node capture Attack in Wireless Sensor Networks using ICmetrics", In IEEE 3rd international conference on Emerging Security Technologies, 2012.

[16] Sarmad Ullah khan, Luciano Lavagno, Claudio Pastrone, "A Key Management Scheme Supporting Node Mobility in Heterogeneous Sensor Network", In IEEE 6th ICET, pp. 364-369, 2010.

[17] T.D.Subash, C.Divya, "Double Hash Function Scheme in Wireless Sensor Networks", In IEEE Information and communication technologies, pp. 88-92, 2011.

[18] 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.

[19] S.H. Jokhio, I.A. Jokhio, A.H. Kemp, "Node capture attack detection and defence in wireless sensor networks", In IEEE IET Jounnals & Magazines, Vol. 2, No. 3, pp. 161-169, 2011.

[20] Yong Wang, Garhan Attebury, and Byrav Ramamurthy, "A survey of security issues in wireless sensor networks", In IEEE Communications Surveys & Tutorials, Vol. 8, No. 2, pp. 02–23, 2006.

Authors' Profiles

Bhavana Butani received his Bachelor`s degree in Information Technology, MIT, Ujjain, Indian 2010. At present she is pursuing M.E. Degree in Computer Science & Engineering from UIT-RGPV, Bhopal, India.

Her research areas are Computer Networks, Wireless Sensor network, Security Attacks in WSN. She is also working on enhancing attacking efficiency of node capture attack in WSN.

Dr. Piyush B. Shukla Dr. Piyush B. Shukla received his Bachelor's degree in Electronics & Communication Engineering, LNCT in 2001, Bhopal, M. Tech (Computer Science & Engineering) in 2005 from SATI, Vidisha, Ph.D. (Computer Science & Engineering) in 2013 from RGPV, Bhopal. M.P. India. He is a member of IACSIT. He has published more than 15 papers in reputated International Journals and 10 papers in International Conferences.

At present, he is working as an Assistant Prof. in Department of Computer Science & Engineering, UIT-RGPV, Bhopal Since July 2007.

Dr. Sanjay C. Silakari Dr. Sanjay C. Silakari received his Bachelor's degree in Computer Science & Engineering from SATI, Vidisha in 1991. M.E. (Computer Science & Engineering) from DAVV, Indore in 1998. Ph.D. (Computer Science & Engineering) in 2006 from B.U. Bhopal (M.P.) India. He is a member of various Acadamic Society.

At present, he is working as Director in UIT-RGPV and Prof. & Head of CSE Department, UIT-RGPV, Bhopal. He has several research publications to his credit in different reputed national and international conferences & journals. He has edited the proceeding of different international conferences including IEEE conference, & also organized & attended several international & national conferences. He is a life member of India Society for Technical Education (ISTE), Computer Society of India (CSI), the Indian Science Congress Association & International Association of Engineers (IAENG), & a member of IEEE and ACM.

How to cite this paper: Bhavana Butani, Piyush Kumar Shukla, Sanjay Silakari,"Optimized and Executive Survey of Physical Node Capture Attack in Wireless Sensor Network", IJCNIS, vol.6, no.11, pp.26-34, 2014. DOI: 10.5815/ijcnis.2014.11.04

