International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.163.07

A Survey on Clone Attack and Malicious Nodes Identification in Wireless Sensor Networks

N. Mohamed Bayas[1], Dr. G. Ravi[2]
[1]Research Scholar in Computer Science
[2]Associate Professor & Head, Department of Computer Science
Jamal Mohamed College (Autonomous)
(Affiliated to Bharathidasan University)
Tiruchirappalli, Tamil Nadu, India

Abstract- Wireless Sensor Network is deployed in unattended and unsecure environments, so it is vulnerable to various types of attacks. One of the physical attacks is a node replication attack (or) clone attack. An adversary can easily capture one node from the network and extract information from the captured node. WSN can be either static (or) mobile, in that centralized and distributed clone attack detection methods are available. To instigate this attack, an adversary only needs to physically capture one node, and after collecting all secret credentials (ID, cryptographic keys, etc.), an adversary replicates the sensor node and deploys one or more clones of the malicious node into the network at strategic positions, damaging the whole network by carrying out many internal attacks. The detection of malicious or hidden nodes in Wireless Sensor Network (WSN) is important for improving the performance of the WSN. A malicious node in wireless sensor networks can be used to create false messages by generating them on their own or by falsifying legitimate messages received from other nodes. Because malicious nodes that create false messages can waste a considerable amount of network resources, it should detect them as early as possible. In this paper we analyze various centralized and distributed protocols in static and mobile environments. In this protocol review and compare their performance. The existing detection schemes classified and comprehensively explore various proposals in each category. Here it will also take a glance at some technical details and comparisons so as to demonstrate limitations of the existent detections as well as effective contributions.

Keywords: Clone Attack, Sensor Nodes, Malicious Nodes, Internal Attacks, Protocols, WSN

I. INTRODUCTION

A Wireless Sensor Network (WSN), which is a distributed and self-organized network, is a collection of independent sensor nodes with limited resources that work together in order to achieve a common goal. WSN has small sensor nodes, consisting of sensing, data processing and communication components. WSN is a collection of a large number of sensor nodes that are densely deployed in harsh environments to accomplish both military and civil applications. WSN normally consists of a base station that can communicate with a number of wireless sensors using a radio link. Data is collected at the wireless sensor node, compressed and transmitted to the base station directly. WSN suffer from many constraints including low computation capacity, little memory, inadequate energy resources, use of insecure wireless communication channels and deployment of sensor nodes in an unattended environment, these constraints make security in WSN a challenge. Different possible attacks on WSN are Selective forwarding attack, Sinkhole attack, Wormholes attack, Sybil attack, hello-flood attack, Acknowledgement spoofing, Sniffing attack, Data integrity attack, Energy drain attack, Black-hole attack, Denial of service attack, Physical attacks, Traffic analysis attack, Privacy violation by attack and clone Attacks [1].

An adversary can capture a sensor node and take out its key information. Once a node is captured, the attacker can reprogram it and generate a clone of a captured node. These clones (or) replicas can be deployed in all network areas. These replica node attacks are very dangerous to the operations of sensor networks. With a single captured sensor node, the attacker can create as many replica nodes as he wants. The replica nodes are forbidden by the adversary but have keying information that allows them to seem like authorized participants in the network. So it is very much hard to detect a clone attack.

WSN can be either static or mobile. In static WSN sensor nodes are deployed randomly and after deployment their positions do not change. In mobile WSN, the sensor nodes can move their own after deployment. Two types of detection techniques available in static WSN are centralized and distributed. In a centralized approach for detecting node replication, when a new node joins the network, it broadcasts a location claim containing its location and identity to its neighbors. One or more of its neighbors then forward this location claim to the base station. With location information for all the nodes in the network, the base station can easily detect any pair of nodes with the same identity but at different locations. The main disadvantage of this approach is that if the base station is malicious or the path to the base station is blocked, adversaries can add any number of replicas in the

network. Distributed approaches for detecting clone nodes is based on location information for a node being stored at one or more witness nodes in the network. When a new node joins the network, its location claim is forwarded to the corresponding witness nodes. If any witness node receives two different location claims for the same node ID, then the existence of clone is detected [1].

An environment in which a large number of sensor nodes are densely deployed and communicate wirelessly with each other over a limited frequency and bandwidth is known as Wireless Sensor Network. These sensor nodes sensed the data and forward it to the base station through multi-hop routing. In WSNs there are two other mechanisms, called "aggregation points" and "base stations", which have extra influential resources than normal sensors where aggregation points collect information from their nearby sensors, integrate them and then forward to the base stations to process gathered data [2].

Generally, there are two kinds of applications for WSNs including, monitoring and tracking; therefore, some of the most common applications of these networks are: military, medical, environmental monitoring, industrial, infrastructure protection, disaster detection and recovery, agriculture, intelligent buildings, law enforcement, transportation and space discovery. Limitations of Wireless Sensor Networks such as limited storage memory, limited resources, cost and battery constrained which makes the network insecure and also their wireless nature makes them very attractive to attacker so security is a necessary requirement for these networks [2].

Wireless Sensor Networks are vulnerable to security attacks due to the broadcasting transmission mediums. Furthermore, wireless sensor networks have probably been collected through direct site surveillance. Relatively, sensor networks strengthen the privacy problem because they make large volumes of data easily available through remote network access. Hence, attackers need not be physically present to maintain a long time. They can gather information at low-risk in an unknown manner. Some of the more common attacks against sensor network privacy are:

- Monitor and Eavesdropping: This is the most common attack on privacy. By intruding the data, the adversary could easily discover the communication node contents. When the routing conveys the control information about the sensor network configuration, which contains probably more detailed information than accessible through the location server, the eavesdropping can act against the security policy effectively.
- Traffic Analysis: Even when the messages transferred are secured, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an intruder to cause malicious harm to the sensor network.
- Camouflage Adversaries: intruders can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to get information from the packets, and then change the path of the packets, conducting the privacy analysis.

The intruder's monitoring listens to and modifies the data stream in the communication channel are known as an active attack. The following attacks are active in nature,

- Denial of Service Attacks,
- Node Subversion,
- Node Malfunction,
- Node Outage,
- Physical Attacks,
- Message Corruption,
- False Node,
- Node Replication Attacks,
- Passive Information Gathering [3].

The rest of the paper is organized as follows. In section II the clone attack detection in wireless sensor network is explained. The Section III a survey on various clone attacks is given. The Section IV presents new ideas to carry out the research in new dimension and ends with conclusion in Section V.

II. CLONE ATTACK DETECTION IN WIRELESS SENSOR NODES

Centralized approach

Some of the protocols available for detecting clone attacks using a centralized approach are discussed in the following paragraph.

SET Protocol

In this protocol, the network is arbitrarily divided into exclusive subsets. Each of the subsets has a subset leader and members. The members are one-hop away from their subset leader. Each subset leader collects member

information and forwards it to the root of the sub-tree. The intersection operation is performed on each root of the sub-tree to detect replicated nodes. If the intersection of all sub-trees is vacant there are no clone nodes in this sub-tree. In the last stage, each root forwards its report to the base station. The base station detects the clone nodes by computing the intersection of any two received sub-trees [4].

Real-Time Detection protocol

Each sensor is preloaded with a code word created from a superimposed S-disjunct code. Then a node can compute its finger-print based on the code words collected from its neighborhood. Each node also computes the finger-prints for its neighbors and stores them for future verification. Whenever a sensor node sends a message to the base station, it includes its finger-print. The base station also retains the finger-print for each sensor node. The false finger-print of the node can be identified by the base station [5].

New protocol

Before node deployment, the base station creates a symmetric polynomial for pair-wise key establishment. Each node belongs to the unique generation through the use of symmetric polynomial. The created cloned nodes also belong to the same generation as a malicious node. A node is newly deployed means it belongs to the new group and establishes as pair-wise keys with their neighbors. An attacker compromising an old deployed node cannot interact with existing nodes in the network, because the cloned nodes will fail to set up a pair-wise key with their neighbors [6].

Compressed sensing Clone Identification (CSI)

Each node broadcasts a fixed sensed data to its one- hop neighbors. Sensor nodes forward and aggregate the received number from successor nodes along the aggregation tree with the base station as the root of the aggregation. The tree receives the aggregated result and recovers the sensed data of the networks. The node with the senor reading greater than the fixed sensed data is a clone [7].

Distributed approach

Some of the protocols using distributed approaches are introduced in the following paragraph.

Broadcast Protocol

Each node in the network uses a genuine broadcast message to flood the network with its location information. Each node stores the location information for its neighbors. If it receives a conflicting claim, it revokes the offending node [8].

Deterministic Multicast (DM) Protocol

Each node shares a node's location claim with a limited subset of deterministically selected witness nodes. A node broadcasts its location claim to its neighbors. They forward that claim to a subset of nodes called witnesses. The witnesses are chosen as a function of the node's ID. If the adversary replicates a node, the witnesses will receive two different location claims for the same node ID. The conflicting location claims become evidence to trigger the revocation of the replicated node [9].

Randomized Efficient and Distributed (RED) Protocol

The base station broadcasts a random value to all nodes in the network. Each node broadcasts a location claim to its neighbors. Then each neighbor selects a witness node to forward the location claim. The witness node selection based on a pseudo-random function with the inputs of node`s ID, the random value which is broadcasted by the base station and the number of target locations. Location claims with the same node ID will be forwarded to the same witness nodes in each detection phase. Hence the clone nodes will be detected in each detection phase. Next time when the protocol executes, the witness nodes will be different since the random value which is broadcasted by the base station is changed [10].

Randomized Multicast (RM) Protocol

In this protocol each node broadcasts its location claim, along with a signature authenticating the claim. Each of the node`s neighbors probabilistically forwards the claim to a randomly selected set of witness nodes. If any witness receives two different location claims for the same node ID it can revoke the replicated node [11].

Line Selected Multicast (LSM) Protocol

In this protocol when a node announces its location, every neighbor first locally checks the signature of the claim and then forwards it to randomly selected destination nodes. A location claim, when travelling from source to destination, has to pass through several in-between nodes that form a claim message path. Node replication is detected by the node on the intersection of two paths generated by two different node claims carrying the same ID and coming from two different nodes [12].

Localized multicast Protocol

1. Single Deterministic Cell (SDC) Protocol

In this protocol the node broadcasts its location claim, each neighbor, first verifies the validity of the signature in the location claim. Each neighbor autonomously decides whether to forward the claim. If a neighbor plan to forward the location claim, it first needs to execute a geographic hash function to determine the destination cell. Once the location claim arrives at the destination cell, the sensor receiving the claim first verifies the legitimacy of the signature.

The location claim is flooded within the destination cell. Whenever any witness receives a location claim with the same identity but a different location compared to a previously stored claim, it forwards both location claims to the base station. Then, the base station will broadcast a message within the network to revoke the replicas [13].

2. *Parallel Multiple Probabilistic Cells (P-MPC)*

In P-MPC the location claim is mapped and forwarded to multiple deterministic cells with various probabilities. When a node broadcasts its location claim, each neighbor independently decides whether to forward the claim in the same way as in the SDC scheme. The neighbors that forward the claim can decide the destination cell based on geographic hash cells to which the identity of the sender is mapped, based on a geographic hash function [14].

Memory Efficient Multicast Protocols

1. Memory Efficient Multicast using Bloom filters (B-MEM) Protocols

This protocol forwards a location claim to randomly selected locations on a line segment. All the midway nodes on the line serve as watchers while the first and last node serves as witnesses. When a node receives the location claim, it performs the two-phase conflict check to detect conflict claims [15].

2. Memory Efficient Multicast using Bloom filters and Cell forwarding (BC- MEM) Protocols

In this protocol the deployment area is divided into virtual cells. In each cell, an anchor point is assigned for every node in the network. The node nearby to the anchor point is called an anchor node. The location claim is forwarded to the anchor point of the next cell where the line segment interacts. The claim is then forwarded from one anchor node to another until it reaches the last cell. The anchor nodes in the in-between cells are watchers and anchor nodes in the first and last cells are witnesses [16].

3. Hierarchical Distributed Algorithm (HDA)

This algorithm has three steps. In the first step all the material required for Bloom filter computations and for cryptographic operations trees hierarchical architecture. These sensor nodes send their data only to their cluster heads. The cluster heads forward them to the base station. Cluster heads communicate with each other through dedicated paths and create a kind of tree with the base station as a root. The detection is performed by the cluster nodes using a Bloom filter mechanism and based on the hierarchical architecture of the wireless sensor networks [17].

Random Walk Based Protocols

Random Walk Based routing is a probabilistic protocol. In this protocol the nodes are selected randomly from their neighbors nodes which will forward the data packet. The resultant path thus generated is a random walk (RW).

1. Random Walk (RAWL)

Each node broadcasts a signed location claim. Each of the node's neighbors probabilistically forwards the claim to some randomly selected nodes. Each randomly selected node sends a message containing the claim to start a random walk in the network. The passed nodes are selected as witness nodes and it will store the claim. If any witness receives different location claims for the same node ID. This will result in the detection of the replicated node [18].

2. *Table Assisted Random walk (TRAWL)*

In this protocol when a randomly chosen node starts a random walk, all the passed nodes will still become witness nodes. However, now they do not definitely store the location claim, instead, they store the location claim independently. Also, each witness node will create a new entry in its trace table for recording the pass of a location claim. When receiving a location claim a node will first find the entries which have the same node ID as the claim in its trace table. Then if any entry is found, the node will compute the digest of the claim and compare the digest with the digest in the entry. When two digests are different, the node detects a clone attack [11].

3. *Detection of Node Capture Attack (DNCA)*

This protocol uses the concept that the physically captured nodes are not present in the network during the period from the captured time to the redeployment time. The captured nodes did not participate in any network operation during this period. The captured node can be identified by the Sequential Probability Ratio Test (SPRT). The protocol then measures the absence time period of a sensor node and compares it to a predefined threshold. If it is more than the threshold value, the sensor node considered as a captured node [10].

4. Cell based Identification of Node Replication Attack (CINORA)

In this method sensor network is divided into geographical cells similar to the existing cellular network. In CINORA-Inset, location claims from the nodes are distributed among a subset of cells to detect any replication. These cells are generated from a non-null intersecting subset algorithm. During the authentication phase at least one cell receives conflicting location claims, if the adversary has ever attempted to replicate legitimate nodes [19].

III. REVIEW OF LITERATURE

P. Uma Maheswari1 P. Ganesh Kumar, 2016 proposed the message verification and passing method for analyzing the trustworthiness or otherwise for detecting the Cloned node. The action of a node as a Cloned node with duplicate information can happen only when the node has complete information about other nodes. Verification of the node needs the application of Position Verification Method. Instead of wasting time for PVM to check each and every node, the message verification and passing procedure is applied for authentication prior to communication. If a node does not have any authorization by the base station, it cannot communicate with any other node in the network. The message verification and passing method is so effective for more time consuming than any other method. Message verification and passing method requires modification and reduction in time consumption and cost-effectiveness. The size of the network is not a constraint. The throughput of the network should be higher than the other security algorithm which is applied earlier in the network security [20].

R.Sathish, D.Rajesh Kumar 2013 found that WSNs are prone to clone attacks that lead to many devastating effects. In a clone attack, an attacker initially captures a node in the network and reprograms the node. In the later stage the adversary replicates the reprogrammed node and spread throughout the network for taking control over the network. There are a few distributed solutions available for this problem. But the issues related to energy and memory demanding in any WSN protocol makes these solutions ineffective. In order to overcome these drawbacks, a lightweight, fast, efficient and mobile agent-based security solution against cloning attack or replication attack is been proposed for WSNs[21].

Swati Raimule1, Anjali Chandavale, 2016 evaluate various detection protocols. RAWL protocol is assumed to be the best protocol considering its simulation results. In the paper, an attempt have been made to improve this protocol, and we come up with a new protocol called Neighbor Division- RAWL (ND-RAWL). This protocol is modified version of existing RAWL protocol. The simulation result shows that the communication cost of our protocol is less as compared to the RAWL. Simulation results demonstrate that proposed protocol achieved very good performance in terms of communication overhead, and message delivery latency, while assuring a high message delivery ratio. We consider the detection of cloned nodes in mobile WSNs as the future work [22].

Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini 2011 presented and justified a few basic requirements an ideal protocol for distributed detection of node replicas should have. In particular, we have introduced the preliminary notion of ID-obliviousness and area-obliviousness that convey a measure of the quality of the node replicas detection protocol; that is, its resilience to a smart adversary. Moreover, we have indicated that the overhead of such a protocol should be not only small, but also evenly distributed among the nodes, both in computation and memory. Further, we have introduced new adversary threat models. However, a major contribution of this paper is the proposal of a self-healing, randomized, efficient, and distributed protocol to detect node replication attacks. The analytical part have compared RED (Randomized Efficient and Distributed (RED) Protocol with the state of- the-art solution (LSM) Line Selected Multicast (LSM) Protocol and proved that the overhead introduced by RED is low and almost evenly balanced among the nodes; RED is both ID-oblivious and area oblivious; furthermore, RED outperforms LSM in terms of efficiency and effectiveness. Extensive simulations confirm these results. Lastly, also in the presence of malicious nodes, we can analytically show that RED is more resilient in its detection capabilities than LSM [23].

Anandkumar K.M1, Jayakumar C2, Arun Kumar P3, Sushma M4 and Vikraman R 2012 presented and justified a few basic requirements for node replication attacks under pervasive health care environments. In particular, we have introduced new adversary threat models. However, a major contribution of this paper is the proposal of a self-healing, randomized, efficient, and distributed protocol to detect node replication attacks. We analytically compared Randomized Efficient Distributed Multicast (REDM) with Secure Randomized Efficient Distributed Multicast (SREDM) and proved that the overhead introduced by RED is high and almost evenly unbalanced among the nodes. Extensive simulations confirm these results. Lastly also in the presence of malicious nodes, we can analytically show that SRED is more resilient in its detection capabilities than RED [24].

Reyaz Ahmad sheikh1, Rajeev kumar Arya2, Mr.ShubhashishGoswami 2014 provides few distributed solutions to address this fundamental problem have been recently proposed. However, these solutions are not satisfactory. Therefore first, the desirable properties of a distributed mechanism for the detection of node Clone attacks have been analyzed. Second, the known solutions for this problem do not completely meet our requirements. Third, a new self healing, RED protocol for the detection of node Clone attacks has been proposed, and it satisfies the intended requirements. The proposed method has been implemented using NS-2. The results of the implementation show that the proposed method is efficient to detect clone attack in the WSN efficiently. Further since the proposed method has signature of containing only four fields the system overheads are low, thereby reducing the energy consumption of the nodes. This further increases the throughput and reduces the delay as compared to methods proposed in the literature [25].

Suresh.H, Ravindra.S.Hegadi 2017 analyzes the desirable properties of a distributed mechanism for the detection of node replication attacks. Second, we show that the known solutions for this problem do not completely meet our requirements. Third, we propose a new self-healing, RED protocol for the detection of node replication attacks, and we show that it satisfies the introduced requirements. Our Implementation specifies user will specify its ID, Location ID, Random number, Destination ID along with Destination Location ID, to the Witness node. The witness will verify the internally bounded user ID with the user-specified ID. If the Verification is Success, the packets are sent to the destination. It proposes Modified RED Scheme to identify Cloning attacks in the Network [26].

Zhongming Zheng†, Anfeng Liu‡, Lin X. Cai§, Zhigang Chen‡, and Xuemin (Sherman) Shen 2013 propose a location-aware clone detection protocol, which guarantees successful clone attack detection and has a little negative impact on the network lifetime. Specifically, we utilize the location information of sensors and randomly select witness nodes located in a ring area to verify the privacy of sensors and to detect clone attacks. The ring structure facilitates energy-efficient data forwarding along the path towards the witnesses and the sink, and the traffic load is distributed across the network, which improves the network lifetime significantly. Theoretical analysis and simulation results demonstrate that the proposed protocol can approach 100% clone detection probability with trustful witnesses. We further extend the work by studying the clone detection performance with untrustful witnesses and show that the clone detection probability still approaches 98% when 10% of witnesses are malicious. Moreover, our proposed protocol can significantly improve the network lifetime, compared with the existing approach [27].

H. Wen1 J. Luo2 L. Zhou 2011 presented a novel scheme to detect the node clone attack in WSN by channel identification characteristic in which the clone nodes are distinguished by the channel responses between nodes. The proposed scheme aims at achieving fast detection and minimizing the data transmission cost by taking advantage of temporal and spatial uniqueness in physical layer channel responses. In contrast to previous solutions, the proposed approaches feature nearly-perfect resilience to node clone attack with low communication and computation costs, low memory requirements and high detection probability [28].

Mohammad Y Aalsalem1, Wazir Zada Khan, N. M. Saad 2015 propose a novel enhancement in RAWL protocol aiming to decrease the communication and memory costs while keeping the detection probability high. Our simulation results show that this improvement in RAWL not only reduces the communication and memory costs but also ensures high security of witness node. Also due to the lack of physical tamper-resistance, an adversary can easily capture and compromise sensor nodes and after replicating them, he inserts an arbitrary number of clones into the network. As a result the adversary is able to mount a wide variety of internal attacks. Several solutions have been proposed in the literature for the detection of these clones from which witness node based distributed solutions have shown satisfactory results. Random Walk (RAWL) is one of the witness nodes based distributed techniques in which witness nodes are randomly selected by initiating several random walks throughout the network. Although RAWL has achieved high security of witness nodes but in accomplishing high detection probability RAWL suffers from very high communication and memory overhead [29].

Guo Cheng∗, SongtaoGuo∗, Yuanyuan Yang‡ and Fei Wang 2015 propose an improved LEACH (NI-LEACH) protocol to reduce the scale of the cluster by considering the residual energy of nodes and the optimal number of clusters. Furthermore, we design an intrusion detection algorithm to detect the replication attacks by introducing monitor nodes in the network so as to greatly reduce the occurrence of tampering with the information. Simulation results show that our proposed algorithm is simple yet efficient. An attacker can be detected with high

probability while achieving approximately optimal throughput. The network's ability against the attack from clone nodes is greatly improved [30].

A Vanathi, B.Sowjanya Rani 2012 propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol (ZKP) for verifying the authenticity of the sender sensor node. The cloning attack is addressed by attaching a unique finger-print to each node that depends on the set of neighboring nodes and itself. The finger-print is attached to every message a sensor node sends. The ZKP is used to ensure non-transmission of crucial cryptographic information in the wireless network in order to avoid Man-in-The Middle (MITM) attack and replay attack. We are extending the previous method and proposed a new method by introducing a work rate measure to detect the cloned node. The security and performance analysis indicate that our algorithm can identify clone attacks with a high detection probability at the cost of a low computation/ communication/storage overhead [31].

Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei 2014 analyze the desirable properties of a distributed mechanism for the detection of node replication attacks. Second, we show that the known solutions for this problem do not completely meet our requirements. Third, we propose a new self-healing, randomized, efficient, and distributed protocol (RED) for the detection of node replication attacks, and we show that it satisfies the introduced requirements. Finally, extensive simulations show that our protocol: Is highly efficient in communication, memory, and computation; is much more effective than competing solutions in the literature; is resistant to the new kind of attacks introduced in this paper, while other solutions are not [32].

PinakiSankar Chatterjee and Monideepa Roy proposed a new method using Cuckoo hashing technique to detect cloned nodes. This technique is applied in maximum-match filtering (MMF) algorithm to provide a good sensing decisions by avoiding the node cloning attack. This technique is space-efficient with less false-positive rate [33].

P.P. Devi and B. Jaison, proposes a new technique called hybrid clone node detection (HCND) using SDN mechanism to eliminate redundant nodes during cloning attack. The various parameters considered in HCND include false positive, false negative ratio analysis, precision analysis, recall analysis and detection analysis [34].

Luo *et al*. have pointed out that infrastructure-less ad hoc networks rarely have a real defense mechanism against most of the attacks, including both outsider and insider attacks such as malicious node attacks. They suggested a system design like this – if one node is named trusted by certain number of its neighboring nodes, that particular node is trusted both locally and globally. However, since the system uses a minimum number of trusted nodes it is not so applicable to sensor networks where the nodes are randomly spread out. In other words, it is possible that under certain conditions nodes cannot find the minimum number of neighboring nodes in order to be named trusted [35].

In a trust-based intrusion detection scheme as in [36], the author has considered a composite trust metric deriving from both social trust (honesty) and QoS trust (energy and cooperativeness) as an indicator of maliciousness. By statistically analyzing peer-to-peer trust evaluation results collected from sensor nodes, each cluster head applies trust- based intrusion detection to assess the trustworthiness and maliciousness of sensor nodes in its cluster. Cluster heads themselves are evaluated by the base station. An analytical model based on stochastic Petrinets is developed for performance evaluation of the proposed trust-based intrusion detection scheme, as well as a statistical method for calculating the false alarm probability. Simulation results show the effectiveness of the approach.

The Neighbor-based intrusion detection method proposed in [37] explores the principle that sensor nodes situated spatially close to each other tend to have a similar behavior. A node is considered malicious if its behavior significantly differs from its neighbors. The author has implemented IDS for the Tiny OS which uses the received signal strength, packet delivery ratio as well as proposed packet dropping ratio and received to sent ratio to detect selective forwarding, jamming and hello flood attacks. They have evaluated the implemented IDS in the TOSSIM simulator. The proposed IDS are capable of detecting the attacks with reasonably low occurrence of false positives and negatives when collaboration among nodes is employed.

IV. PROBLEM IDENTIFICATION

- WSN is deployed in unattended and insecure environments, so it is vulnerable to various types of attacks.

- One of the physical attacks is a node replication attack (or) clone attack. An adversary can easily capture one node from the network and extract information from the captured node.
- All the above-mentioned methods and protocols are highly complex due to its complicated components. (All the techniques and protocols which are discussed in this survey is implemented)
- An adversary can misuse this protocol to revoke original nodes.
- Real-Time protocol cannot handle a sophisticated replica which can compute by itself a finger-print consistent with its neighborhood.
- In New protocol the sensor nodes are bound to their groups and geographic locations.
- The Broadcast protocol have high communication and memory cost for large sensor networks.
- The Deterministic Multicast (DM) protocol not provided much security, the adversary easily compromise witness nodes.
- The node in the network that first receives the location claim is unable to distinguish between claims of original and cloned node. This has much higher detection probability and communication overhead.

V. CONCLUSION

Wireless Sensor Networks are used in many applications like military, health and commercial applications but due to some limitations in WSNs like minimal energy and storage and due to deployment of sensor nodes in an unattended environment makes very attractive to the attacker so it is necessary to secure the network from attacks. This paper summarizes the classification of attacks, identification of malicious nodes and the explanation of how these attacks arise in the network. There is a survey on various detection centralized and distributed schemes for detecting the clone attack and this prompt future researcher to come up with more security mechanisms for detection of clone attack and make their system safer.

REFERENCES

[1] J.Anthoniraj, T.AbdulRazak, "Clone Attack Detection Protocols in Wireless Sensor Networks: A Survey" *International Journal of Computer Applications,* (0975 – 8887) Volume 98– No.5, July 2014.
[2] Avneet Kaur1, P. S. Mann, "DETECTION OF CLONE ATTACKS IN WIRELESS SENSOR NETWORKS: A SURVEY", *IJCAR*, vol-2, issue: 3, March 2014.
[3] Amanpreet Kaur Sidhu1, Dinesh Kumar, " Node Replication Attack in Wireless Sensor Networks: A Survey", ISSN-2321 -3361 © *IJESC*, 2015
[4] Cris Townsend, Stevan Arms, "Wireless sensor network: principles and applications", Chapter 22, pp439-449.
[5] Dr.G.Padmavathi, Mrs.D.ShanmugaPriya, "A Survey of attacks, security mechanisms and challenges in wireless sensor networks", *International Journal of computer science and information security*, vol.4, no.1&2, 2009.
[6] PrabhuduttaMohanty, SangramPanigrahi, NityanandaSarma and Siddhartha SankarSatapathy, "Security issues in wireless sensor network data gathering protocols: A Survey", *Journal of Theoretical and Applied Information Technology*, pp14-29, 2005-2010.
[7] Mona Sharifnejad, Mohsen sharifi, MansourehGhiasabadi and surehBeheshti. "A Survey on Wireless Sensor Networks Security", Fourth International Conference: *Sciences of Electronic Technologies of Information and Telecommunication*, March 25-29, 2007
[8] Yan-Xiao Li, Lain-Qin, Ian-Liang, "Research on wireless Sensor network security", *IEEE Computer Society*, International Conference on Computational Intelligence and Security, 2010.
[9] Jun-Won Ho, Dogging Lin, Matthew Wright, SajaiK.Das "Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks", *Preprint submitted Elsevier*, March 2009.
[10] Bio Zhu, Sanjeev Setia, SushilJajodia, Sankardas Roy and Lingyu Wang "Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks", *IEEE Transactions on Mobile Computing*, Vo1 9, No 7, Pages 913-926, July 2010
[11] Bio Zhu, Venkata Gopala Krishna Addada, Sanjeev Setia, SushilJajodia and Sankaradas Roy, "Efficient Distributed Detection of Node Replication Attacks in sensor Networks", *IEEE Computer Society*, 23 rd Annual Computer Security Applications Conference,Pages 257 – 266, 2007
[12] Hesiod Choy, Cancun Zhu and T.F.La Porta," SET: Detecting Node clones in Sensor Networks", Proc of 3rd International Conference on Security and Privacy in comm...Networks (*Secure Comm*) Pages 341-350, 2007
[13] Kai Xing,FangLiu,XiuzhenCheng,DavidH.C.Du," Real-time Detection of clone attacks in Wireless Sensor Networks", *IEEE ICDCS*, 2008
[14] C. Bekara and M. Laurent- Maknavicius,"A New Protocol for securing Wireless Sensor Networks against nodes replication attacks, *"Third IEEE International Conference on Security and Privacy in communication networks*, 2008
[15] C.M.Yu, C.S.Lu and S.Y.Kuo,"CSI: Compressed sensing based clone identification in sensor networks"in proceedings of the *IEEE International conference on pervasive computing and communications workshops*, pages 290-295, March-2012
[16] Bryan Parno, Adrian Perrig, Virgil Gligor, " Distributed Detection of Node Replication Attacks in Sensor Networks ", In proceeding of the *IEEE Symposium on Security and Privacy* , 2005
[17] Mauro Conti, Roberto Di Pieto, L.V.Mancini and A.Mei,"A Randomized and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks ", *Proc.ACMMobiHoc*, Pages 80-89, Sept 2007
[18] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini and Alessandro Mei "Distributed Detection of Clone Attacks in Wireless Sensor Networks" *IEEE Transactions on Dependable and Secure Computing*, Vol 18, No 5, Pages 685-698, September/October 2011
[19] Ming Zhang, Vishal Khanapure, ShigangChen,Xuelian Xiao, "Memory Efficient Protocols for Detecting Node Replication Attacks in Wireless Sensor Network" *IEEE*, Pages 284-293, 2009.
[20] P. Uma Maheswari1, P. Ganesh Kumar2," Dynamic Detection and Prevention of Clone Attack in Wireless Sensor Networks", *Springer Science+Business Media,* New York 2016.

[21] R.Sathish,D.Rajesh Kumar, "Dynamic Detection of Clone Attack in Wireless Sensor Networks, 2013 International Conference on *Communication Systems and Network Technologies*.

[22] Swati Raimule1, Anjali Chandavale, "A New Approach to Detect Clone Attack in WSN", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, Web Site: www.ijettcs.org Email: editor@ijettcs.orgVolume 5, Issue 4, July - August 2016.

[23] Mauro Conti, Member, IEEE, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks", *IEEE Transactions on Dependable and Secure Computing*, VOL. 8, NO. 5, SEPTEMBER/OCTOBER 2011

[24] Anandkumar K.M1, Jayakumar C2, Arun Kumar P3, Sushma M4 and Vikraman R, "INTRUSION DETECTION AND PREVENTION OF NODE REPLICATION ATTACKS IN WIRELESS BODY AREA SENSOR NETWORK", *International Journal of UbiComp (IJU)*, Vol.3, No.3, July 2012

[25] Reyaz Ahmad sheikh1, Rajeev kumar Arya2, Mr.ShubhashishGoswami, " Detection of Clone Attack in Wsn" *IOSR Journal of Computer Engineering (IOSR-JCE)*, e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. V (Sep – Oct. 2014), PP 48-52 www.iosrjournals.org.

[26] Suresh.H,Ravindra.S.Hegadi, "MODELING AND DETECTION OF DISTRIBUTED CLONE ATTACKS FOR SAFETY TRANSACTIONS IN WSN" *International Journal of Contemporary Research in Computer Science and Technology (IJCRCST)*, *e*-ISSN: 2395-5325 Volume 3, Issue 1 (January '2017)

[27] Zhongming Zheng†, Anfeng Liu‡, Lin X. Cai§, Zhigang Chen‡, and Xuemin (Sherman) Shen, "ERCD: An Energy-efficient Clone Detection Protocol in WSNs", *IEEE*, 978-1-4673-5946-7/13/$31.00 ©2013.

[28] H. Wen1 J. Luo2 L. Zhou, "Lightweight and effective detection scheme for node clone attack in wireless sensor networks", *IET Wirel. Sens. Syst.,* 2011, Vol. 1, Iss. 3, pp. 137–143

[29] Mohammad Y Aalsalem1, Wazir Zada Khan, N. M. Saad, "Detecting Clone in Wireless Sensor Networks Using Constrained Random Walk", *International Conference on Radar, Antenna, Microwave Electronics and Telecommunications,* 2015.

[30] Guo Cheng∗, SongtaoGuo∗, Yuanyuan Yang‡ and Fei Wang, "Replication Attack Detection with Monitor Nodes in Clustered Wireless Sensor Networks", *IEEE,* 978-1-4673-8590-9/15/$31.00, ©2015.

[31] A Vanathi, 2B.Sowjanya Rani, "Cloning Attack Authenticator in Wireless Sensor Networks", *IJCST,* Vol. 3, Issue 1, Spl. 5, Jan. - March 2012

[32] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks" *IEEE,* 1545-5971/10/$26.00, © 2010.

[33] PinakiSankar Chatterjee and Monideepa Roy, "Lightweight cloned-node detection algorithm for efficiently handling SSDF attacks and facilitating secure spectrum location in CWSNs", *IET Wirel. Sens. Syst.,* 2018, Vol. 8 Iss. 3, pp. 121-128.

[34] P.P. Devi and B. Jaison, "Protection on Wireless Sensor Network from Clone Attack using the SDN-Enabled Hybrid Clone Node Detection Mechanisms", *Computer Communications*, Volume 152, 15 February 2020, Pages 316-322.

[35] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, Lixia Zhang, "Self-securing Ad Hoc Wireless Networks," *IEEE ISCC (IEEE Symposium on Computers and Communications,)* 2002.

[36] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, Jin-Hee Ch, "Trust-Based Intrusion Detection in Wireless Sensor Networks", *IEEE International Conference on Communications (ICC)*, 2011, pp. 1-6.

[37] Andriy Stetsko, Lukas Folkman, Vashek Matyas, "Neighbor-based Intrusion Detection for Wireless Sensor Networks", 6th *International Conference on Wireless and Mobile Communications (ICWMC)*, 2010, pp. 420-425