Clone Attack Detection Protocols in Wireless Sensor Networks: A Survey

J.Anthoniraj
Research Scholar
Bharathidasan University, Trichy

T.Abdul Razak
Associate Professor
Jamal Mohamed College, Trichy

ABSTRACT
Wireless Sensor Network (WSN) is a collection of autonomous sensor nodes which are low cost hardware components consists of sensor nodes with constraints on battery life, memory size and computation capabilities to monitor physical (or) environmental conditions. WSN is deployed in unattended and unsecure environments, so it is vulnerable to various types of attacks. One of the physical attacks is node replication attack (or) clone attack. An adversary can easily capture one node from the network and extract information from captured node. Then reprogram it to create a clone of a captured node. Then these clones can be deployed in all network areas, they can be considered as legitimate members of the network, so it is difficult to detect a replicated node. WSN can be either static (or) mobile, in that centralized and distributed clone attack detection methods are available. In this paper we analysis various centralized and distributed protocols in the static and mobile environments. We review these protocols and compare their performance with the help of witness selection, communication and memory overhead, detection probability of replicated nodes, resilience against adversary's node compromise.

General Terms
Clone attack, Clone attack detection approach, Static nodes, and Mobile nodes.

Keywords
Security attack, Base Station, Clone attack, Clone attack detection, Centralized approach, Distributed approach.

1. INTRODUCTION
A Wireless Sensor Network (WSN), which is 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 [1].WSN has small sensor nodes, consisting of sensing, data processing and communication components [2].WSN is a collection of large number of sensor nodes that are densely deployed in harsh environment to accomplish both military and civil applications [3]. 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 [4]. 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[2,5]. 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[6,7,8].

The rest of this paper is organized as follows. Section 2 describes about clone Attack. In section 3, we have discussed clone attack detection methods. In section 4, we summarize the existing

Centralized and distributed detection protocols used to detect clone nodes in static sensor networks. In section 5, we present various protocols to detect clone attacks for mobile WSNs. We present a comparison between these protocols in section 6.The main drawbacks of these protocols are listed in section 7.Finally section 8 presents the concluding remarks.

2. CLONE ATTACK
An adversary can capture a sensor node and take out its key materials. 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 materials that allow them to seem like authorized participants in the network. So it is very much hard to detect a clone attack [9].

3. CLONE ATTACK DETECTION
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 compromised or the path to the base station is blocked, adversaries can add any number of replicas in the network [10].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 [11].Some of the protocols to detect clone attack in static sensor networks are introduced in the following paragraph.

4. CLONE ATTACK DETECTION IN STATIC SENSOR NODES

4.1 Centralized approach

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

4.1.1 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 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 [12].

4.1.2 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 [13].

4.1.3 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 compromised 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 pair-wise key with their neighbors [14].

4.1.4 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 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 [15].

4.2 Distributed approach

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

4.2.1 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 [16].

4.2.2 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 an evidence to trigger the revocation of the replicated node [16].

4.2.3 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 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 [17].

4.2.4 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 forward 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 [16].

4.2.5 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 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 [18].

4.2.6 Localized multicast

4.2.6.1 Single Deterministic Cell (SDC)

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 plans 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 [19].

4.2.6.2 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 a geographic

hash cells to which the identity of the sender are mapped, based on a geographic hash function [20].

4.2.7 Memory Efficient Multicast Protocols

4.2.7.1 Memory Efficient Multicast using Bloom filters (B-MEM)

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 serve as witnesses. When a node receives the location claim, it performs the two-phase conflict check to detect conflict claims [21].

4.2.7.2 Memory Efficient Multicast using Bloom filters and Cell forwarding (BC- MEM)

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 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 at the last cell. The anchor nodes in the in-between cells are watchers and anchor nodes in the first and last cells are witnesses [21].

4.2.8 Hierarchical Distributed Algorithm (HDA)

This protocol has three steps. In the first step all the material required for Bloom filter computations and for cryptographic operations tree hierarchical architecture. In These sensor nodes send their data only to their cluster heads. The cluster heads forward them to the base station. Cluster heads communicate each other through dedicated paths and create a kind of tree with 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 [22].

4.2.9 Random Walk Based Protocols

4.2.9.1 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 a same node ID. This will result in the detection of the replicated node [23].

4.2.9.2 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 digest are different, the node detects a clone attack [23].

4.2.10 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 not participate in any network operation during this period. The captured node can be identified by SQRT. The protocol then measures the absence time period of a sensor node and compares it to a predefined threshold. If it is more than threshold value, the sensor node considered as a captured node [24].

4.2.11 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 claim 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 adversary has ever attempted to replicate legitimate nodes [25].

5. CLONE ATTACK DETECTION IN MOBILE SENSOR NODES

For static sensor network many different node replication attack detection schemes are used. But in mobile sensor network nodes are moving continuously in the network, techniques for detecting duplicate nodes in static sensor network is not applicable. As a result some protocols developed for mobile WSN to detect the clone attack.

5.1 Centralized Approach

5.1 Fast Detection using SQRT

Each time a mobile sensor node moves to a new location, each of its neighbor asks for a signed claim containing its location and time information and decide probabilistically whether to forward the received claim to the base station. The base station computes the speed from every two consecutive claims of a mobile node and performs the SQRT by taking speed as an observed sample. Each time maximum speed is exceeded by the mobile node, it will expedite the random walk to hit (or) cross the upper limit and thus lead to the base station accepting the alternate hypothesis that the mobile node has been replicated [26].

5.2 Distributed Approach

5.2.1 Extremely Efficient Detection (XED)

In this protocol once two sensor nodes, si and sj are within the communication ranges of each other, they first generate random numbers and then they exchange their random numbers. They also use a table to record the node ID, the generated random number, and the respective memory.

Note that for the pair of two nodes met before the above procedure is also performed such that the random number stored in the memory is replaced by the received random number. The sensor node si meets another sensor node sj. If si never meets sj before, they exchange random numbers otherwise the sensor node si request the sensor node sj for the random number exchanged at earlier time, For the sensor node si, if the sensor node sj cannot replies or replies a number which does not match the number in si's memory, si announces the detection of a replica [27].

5.2.2 Neighbor Based Detection Scheme (NBDS)

In this protocol when a node moves to another location, node should broadcast a rejoining claim to its new neighbors for rejoining the network. Upon receiving the rejoining claim, each new neighbor first verifies the signature. If the signature verification is passed, each new neighbor independently forwards the rejoining claim to a randomly selected node. Once the rejoining claims arrive at destination nodes, the nodes receiving the rejoining claim first verify the validity of the signature and then check if ID is in the neighbor table. If

ID is not in the neighbor table, the nodes receiving the rejoining claim send a report to the Base station for handling this problem [28].

5.2.3 Efficient and Distributed Detection (EDD)

In this protocol the node has mobility and move according to the random way point model. Each node randomly chooses a destination point in the sensing field and then moves toward it. After reaching the destination point, the node remains static for a random time and then starts moving again according in the same rule [29].

5.2.4 Unary Time Location Storage and Exchange (UTLSE)

This protocol has each node initialized with a unique tracking set, which indicates the node is a witness of each node in that track set. When a node encounters a new neighbor, and if that neighbor is in its tracking set, it sends a request for asking that neighbor to send a time-location claim to it. In the meantime, if the node has the same tracked nodes as those neighbors and if the ID is bigger than that neighbor, it sends all the stored time-location claims of each common tracked node to that neighbor. If any witness receives two contradictory time-location claims for the same node ID, it announces that it has successfully detected a replica and triggers a revocation procedure for the given node ID [30].

5.2.5 Single Hop Detection (SHD)

This protocol consists of two phases. In the finger print claim phase each node is required to sign its neighbor node list. This list is broadcasted to its one hop neighbors. The receiver decides whether to become a witness node of the claim node. When it becomes a witness it verifies the list and stores it for future verification. When two nodes meet with each other they exchange their witnessed node list. They can be verified, if the finger print conflicts replica can be identified [31].

5.2.6 Patrol Detection for Replica Attack (PDRA)

In this mobile nodes as patrollers to detect replica distributed in different zones in a network. If a mobile node moves with a speed higher than the denoted maximum speed, it will be regarded as a replicated detection [32].

6. COMPARISION OF PROTOCOLS

Table 1. Notations and Significance

n	Number of nodes in the network
g	Number of witnesses selected by each neighbor
d	Average degree of each node
s	Number of nodes in a cell
l	The node sending the location claim
w	The number of the witness nodes that store the local claim
r	Communication Radius.
N	Number of cluster heads
k	Average number of line segments for each claim
t	Size of a location claim
t^1	The number of bytes that a Bloom filter uses to record the membership of an element.

Table 1 represents various notations used in Table 3, Table 4. The Table 2 classified the protocols according to their type, approach and scheme.

6.1 Witness node Selection

RM protocol distributes location claims to randomly selected set of witness nodes [16]. In LSM protocol a location claim, when travelling from source to destination has to pass through several in-between nodes.LSM was developed as a less expensive version of RM, but it suffers from uneven distribution of witness nodes [18]. RED is similar in principle, to the RM protocol but with witnesses chosen pseudo randomly based on a network-wide seed [17].

In SDC, P-MPC protocols the witness nodes for a node identity are randomly selected from the nodes that are located within a geographically limited region [10]. In P-MPC the location claim is forwarded to multiple deterministic

Table 2. Comparison of Protocols

No	Protocol	WSN Type	Type of approach used	Type of Scheme used
1	SET	Static	Centralized	Base station based
2	Real Time	Static	Centralized	Neighbor based
3	New	Static	Centralized	Group based
4	CSI	Static	Centralized	Base station based
5	Broadcast	Static	Distributed	Network broadcast
6	DM	Static	Distributed	Witness based
7	RED	Static	Distributed	Witness based
8	RM	Static	Distributed	Witness based
9	LSM	Static	Distributed	Witness based
10	SDC	Static	Distributed	Witness based
11	P-MPC	Static	Distributed	Witness based
12	B-MEM	Static	Distributed	Witness based
13	BC-MEM	Static	Distributed	Witness based
14	HDA	Static	Distributed	Cluster based
15	RAWL	Static	Distributed	Witness based
16	TRAWL	Static	Distributed	Witness based
17	DNCA	Static	Distributed	Base station based

18	CINORA	Static	Distributed	Group based
19	Fast	Mobile	Centralized	SQRT based
20	XED	Mobile	Distributed	Conflict based
21	NBDS	Mobile	Distributed	Node mobility
22	EDD	Mobile	Distributed	Node mobility
23	UTLSE	Mobile	Distributed	Time-location based
24	SHD	Mobile	Distributed	Neighbor based
25	PDRA	Mobile	Distributed	Patroller based

Cells with various probabilities by executing a geographic hash function [28]. B-MEM stores the information about a location claim allows randomly selected line segments, which are likely to pass the center area of the deployment [21].BC-MEM does not forward a claim on the line segment. It forwards the claim to the anchor point in the next cell that the line segment intersects. RAWL starts several random walks randomly in the network for each node a. Then it selects the passed nodes as the witness nodes of node a [23]. In NBDS, the neighbors of a rejoining node correspond to the reporters, while the previous neighbors play the role of witnesses [28].

6.2 Communication Overhead

Table 3 represents communication costs used in various distributed clone attack detection protocols. In SET protocol the message authentication codes used for additional security resulted in higher detection cost in terms of communications protocol used the concept of compressed sensing for the identification of clones, so it has lower communication overhead[12]. The Broadcast protocol offers the simplest solution, but the communication overhead will only be tolerable for small network.

DM improves on the communication requirements, by selecting a fixed set of witnesses. RM imposes communication overhead equal to that of the broadcast scheme [29]. The LSM scheme reduces the communication overhead of the RM scheme by having every claim-relaying node participate in the replica detection and revocation process. RED still has the same communication overhead as the LSM scheme [24].

Table 3. Communication Cost

S.No	Protocol	Communication cost
1	SET	O(n)
2	New	O(√n)
3	Broadcast	$O(n^2)$
4	DM	O(gln.g√n/d)
5	RED	O(r.√n)
6	RM	$O(n^2)$
7	LSM	O(n√n)
8	SDC	O(r.√n)+O(s)
9	P-MPC	O(r.√n)+O(s)
10	B-MEM	O(kn√n)
11	HAD	$O(N^2)$
12	RAWL	O(√nlogn)
13	TRAWL	O(√nlogn)
14	DNCA	O(n √n)
13	NBDS	O(r√n)
15	Fast	O(n √n)
16	XED	O(1)
18	EDD	O(1) / O(n)
19	UTLSE	O(n)
20	PDRA	O(n)

The communication overhead of SDC and P-MPC wills only slightly higher that of RED in particular when the network size is large. SDC has the lowest communication overhead though the differences between SDC, P-MPC and LSM are relatively small. As the network size increases P-MPC and SDC have lower overhead than LSM [7]. NBDS has lower communication cost than RM, LSM, SDC, P-MPC protocols [28]. In XED only constant communication cost is required for replica detection. The communication overheads of RAWL, TRAWL, protocols are higher than LSM [23].

6.3 Memory overhead

Table 4 represents communication costs used in various distributed clone attack detection protocols. For networks in which the number of nodes is less than the square of the average degree, RM will tend to be more space efficient [16]. LSM requires storing a higher number of messages compared to RED, because in LSM, every node in a claim path is a possible witness, and therefore, has to store every claim it relays. In RED, only destinations can be witnesses, and thus, only destination is required to store the claims [18]. The memory overhead of the SDC is much lower than those of the RM and LSM protocols [20].

In LSM, a node stores a complete copy of each location claim it receives, some nodes may have to store several hundred location claims, which will exhaust their memory space. In B-MEM, BC-MEM protocols, a node exploits bloom filters to record the foot print of most location claims it receives and it only stores a few complete claims [21]. TRAWL used to reduce the memory overhead of RAWL by using a table to cache the digests of location claims [23].

Table 4. Memory Cost

S.No	Protocol	Memory cost
1	New	O(1)
2	Broadcast	O(d)
3	DM	O(g)
4	RED	O(r)
5	RM	O(√n)
6	LSM	O(√n)
7	SDC	W
8	P-MPC	W
9	B-MEM	O(tk+tk√n)
10	HDA	O(N)
11	RAWL	O(√nlogn)
12	TRAWL	$O(1)^2$
13	DNCA	O(n)
14	NBDS	O(r)
15	Fast	O(n)
16	EDD	O(n)
17	UTLSE	O(√n)

6.4 Detection of Replicated Nodes

SET protocol reduces the detection overhead by computing set operations. The LSM protocol is similar to RM, but it introduces a remarkable improvement in terms of detection probability. RED has better detection probability and converges faster than LSM for all practical values of the network parameters [18]. Compared to the RM and LSM algorithms, a major advantage of SDC is that it ensures more success rate for detecting any node replication [20]. BC-MEM has a slighting lower detection probability than LSM in some cases due to false positive of Bloom filters. BC- MEM achieves a higher detection probability than both LSM and B-MEM by using the cell forwarding technique [21]. HDA have more efficient detection probability than RM and LSM [22].A unique feature of XED is that each node is capable of detecting replicas per move which contrasts sharply with other protocols that need to mobilize the whole network for replica detection[27]. The probability of detecting replicated nodes in NBDS is much higher than RM, LSM protocols. TRAWL has nearly the same probability of defection with RAWL [33].

6.5 Resilience against Node compromise

DM select a fixed set of witnesses, adversary easily compromise witness nodes so it lose resiliency. RM provide excellent resiliency, since it prevents the adversary from anticipating the identity of the witnesses. Finally LSM provides comparable (or) greater resiliency [16]. RED is more resilient in its detection capabilities than LSM [18]. In SDC witness nodes are chosen randomly from the nodes of a given cell instead of the whole network as in the RM protocol .Therefore assuming that the adversary`s capability of compromising nodes is limited. So that in SDC the probability that an adversary can compromise all the witness nodes storing the location claim of a given identity is higher than of the RM protocol. Compared to SDC, P- MPC is more robust to node compromise [20].

7. DRAWBACKS OF THE PROTOCOLS

The SET protocol is highly complex due to its complicated components. An adversary can misuse this protocol to revoke original nodes [12]. Real Time protocol cannot handle a sophisticated replica which can compute by itself a finger print consistent with its neighborhood [13]. In New protocol the sensor nodes are bound to their groups and geographic locations [14]. The Broadcast protocol have high communication and memory cost for large sensor networks. The DM protocol not provide much security, adversary easily compromise witness nodes [16]. Both RM and LSM are unable to detect masked replication attacks [18]. The SDC protocol flooding only the first copy of a node location claim arrives at the cell and the other copies are ignored. The node in the cell that first receives the location claim is unable to distinguish between claims of original and cloned node [10]. In RED protocol the deterministic selection of witness nodes and that infrastructure for distributing random seed may not always be available [17]. The RAWL and TRAWL protocols have much higher detection probability and communication overhead than LSM [23]. The Fast protocol use much more expensive equipment called as GPS. It cannot affordable for the current generation of wireless sensor networks [26]. The XED protocol assumed that the replicas cannot communicate each other, suppose replicas communicate each other then they can establish secret channels among each other and they can easily deceive the detection technique [27]. The EDD protocol is inapplicable due to high storage over head for large scale WSNs [29].

8. CONCLUSION

Wireless sensor networks are deployed in hostile environment and vulnerable to various types of attacks. This paper outlined the different types of attacks on WSN and mainly about clone attack. We have provided various approaches to find the cloned node. In static centralized protocols, CSI protocol has the lowest communication overhead than SET, Real Time, New protocols. In static distributed protocols, we find that SDC protocol has lower communication cost than other protocols for smaller size network and RED protocol has the lowest communication overhead for larger network. The SDC protocol has lower memory overhead than other distributed protocols. The RED and BC-MEM protocols have better detection probability than other protocols. The P-MPC protocol has more resilience against node compromise than other protocols.

9. REFERENCES

[1] T.Bonact,P.Lee,L.Bushnell and R.Poovendra, "Distributed clone detection in wireless sensor networks: an optimization approach ",in Proceedings of the 2nd IEEE International Workshop on Data security and Privacy in Wireless Networks ,Lucca,Italy,June 2011.

[2] Yong Wang,Garhan Attebury and Byrav Ramamurthy "A survey of security networks issues in wireless sensor networks"IEEEcommunicationsSuveysandTutorials,vol.8. no.2,2006.

[3] Ian F.Akyildiz, William Su, Yogis S.Subramaniam and Real Cayirci, "A survey on sensor network", IEEE Communications Magazine, pp 102-114, August 2002.

[4] Cris Townsend, Stevan Arms, "Wireless sensor network: principles and applications", Chapter 22, pp439-449.

[5] Dr.G.Padmavathi, Mrs.D.Shanmuga Priya, "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] Prabhudutta Mohanty, Sangram Panigrahi, Nityananda Sarma and Siddhartha Sankar Satapathy, "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, Mansoureh Ghiasabadi and sureh Beheshti. "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, Sushil Jajodia, 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, Sushil Jajodia 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,Fang Liu,Xiuzhen Cheng,David H.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.ACM MobiHoc, 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] Bio Zhu, Sanjeev Setia, Sushil Jajodia, 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

[20] Bio Zhu, Venkata Gopala Krishna Addada, Sanjeev Setia , Sushil Jajodia 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

[21] Ming Zhang, Vishal Khanapure, Shigang Chen,Xuelian Xiao, "Memory Efficient Protocols for Detecting Node Replication Attacks in Wireless Sensor Network" IEEE Pages 284-293, 2009

[22] Wassim Znaidi, Marine Minjer, Stephane Uheda,"Hierachical Node Replization Attacks Detection in Wireless Sensors networks "IEEE, Pages 82-86, 2009.

[23] Yingpei Zeng, Jiannong Cao, Shigeng Zhang,Shanqing Gao and Li Xie "Random Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks ", IEEE Journal on selected areas in communications, vol 28, No.5 Pages 677-691, June 2010

[24] J.W.Ho,"Distributed detection of node capture attack inwireless sensor networks", in smart wireless sensor networks, pages 345-360, 2010

[25] Y.Lou,Y.Zhang and S,Liu,"Single hop detection of node clone attacks in mobile wireless sensor networks",in Proceedings of the International Workshop on Information and Electronics Engineering (IWIEE)2012.

[26] J.Ho, M.Wright and S.K.Das,"Fast Detection of Replica Node Attacks in mobile sensor networks using sequential analysis", Proc IEEE INFOCOM, Apr 2009

[27] Chia-Mu yu, Chun-shien Lu and Sy Yen Kuo,"Mobile Sensor Network Resilient I against Node Replication Attacks", IEEE, Pages 597-599, 2008

[28] Lee-Chun Ko, Hung-Yuan Chen, Guan-Rong Lin,"A Neighbor-Based Detection Scheme for Wireless Sensor Networks Against Node Replications Attacks",IEEE , 2009

[29] Chia-MuYu, Chun-ShienLu and Sy-Yen Kuo," Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks", IEEE, 2009

[30] Xiaoming Deng, Yan Xiong, Depin Chen,"Mobility-assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks ", IEEE 6th international conference on Wireless and Mobile Computing, Networking and Communications, 2010

[31] Y.Lou,Y.Zhang and S,Liu,"Single hop detection of node clone attacks in mobile wireless sensor networks",in Proceedings of the International Workshop on Information and Electronics Engineering (IWIEE)2012.

[32] L.M.Wang and Y.Shi,"Patrol detection for replica attacks on wireless sensor networks", vol 11, pages 2496-2504, 2011.

[33] Wen Tao zhu, "Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme", International Conference on Network Computing and Information Security, Pages 156-160, 2011