Improved Centralized Base Station Mechanism to Detect Replicas or Clone nodes in Static Wireless Sensor Network

N.S.Usha, E.A.Mary Anita

Abstract: ***The Wireless Sensor Networks offers a wide range of applications due to the high sensing and processing speed of sensor nodes. Since sensor nodes are often deployed in a hostile, unattended, unsafe environment, they are susceptible to many sensible attacks. One such attack is a replication attack or Clone node or identity attack, is a type of insidious attack in which the attacker captures an authentic node, extracts from it all secret credentials and generates replicas identical to the original. These replicas are then used to disrupt its normal functionality by the attacker during the network setup. Several studies have provided many methods to curb replicas, but wireless communication remains an enormous challenge. Our proposed model defines a new mechanism, namely BS-SECCISRNNA (Secure Key Exchange Combined Clone Identification & Secure Neighbour Node Authentication Base Station). This method provides an efficient and quicker identification of clones at multiple locations in the network over a shorter period of time. Simulation results show that our proposed schemes can identify clones simultaneously at multiple locations and define an alternate path for future data transmission.***

Keywords: ***Wireless Sensor Network, Clone node, Detection, Key distribution.***

I. INTRODUCTION

The Wireless Sensor Network comprises of hundreds or thousands of sensor nodes. These sensor nodes are tiny, low cost devices that are self –organizing in nature, relies on battery power and also has some power constraints and limitations of memory and computational capacity. The sensor nodes are mainly deployed to sense the environmental conditions such as temperature, pressure, climatic conditions, soil fertility, moisture, motion, natural calamity, etc. The sensor nodes gather information and exchange with their neighbours in a multihop fashion till it reaches the sink or the data center node. Hence secure routing of data from sensor-sensor nodes to sink node is mandatory [1]-[3].

As sensor nodes are majority employed for Battlefield Surveillance, utmost care must be taken to secure reach of data. Sensor nodes are also used to monitor factory instrumentation, pollution levels, freeway traffic, and structural integrity of buildings. They also monitor firearm discharge, drug or weapon smuggling, illicit crop cultivation, human trafficking, nuclear emissions in rogue region and other illegal activities.

Often, sensor nodes are non-tamper proof; hence there is a possibility of many insider attacks on them. One such attack is the Node replication attack or Clone attack or Identity attack. Here an adversary tries to capture one node, copy all the credentials and cryptographic information and create one or more Clones that are accepted as legitimate nodes by the network. The adversary places these clones at strategic position to monitor or disrupt the network functionality.

Wireless Sensor Networks provide a wide range of solutions to many real-world challenges, but still they suffer from security issues, as the nodes lack hardware support for tamper resistance, as its very costly to implement for hundreds or thousands of nodes. Also the sensor nodes are deployed in unattended environments where the human intervention is highly impossible, thereby making them vulnerable to capture or compromise attacks by an adversary. An adversary can launch a wide variety of physical attacks such as a Node replication attack, Signal or radio jamming attack, Denial of Service attack (DOS), eavesdropping, node outage, Sybil attack, sink hole attack, Selective forwarding attack, worm hole attack etc.

Attacks on Wireless Sensor Network can be classified into two main categories, namely Layer-dependent attacks and Layer-independent attacks [8], which can be further classified as Active and Passive attacks.

In Active attacks, the attacker tries to modify or update or inject data to the message transmitted in the network. The attacker can also inject his/her own message to disrupt the normal operation of the network or cause denial of service attack. In Passive attack, the attacker can only listen to the traffic, analyse the type of data transmitted in the network. This type of attack can be analysed easily, but its difficult to detect.

The Layer-dependent attacks shown in Figure 3 are specific to different OSI layers and they often disrupt specific network functionalities. Some of them are Routing attacks, Data aggregation attacks, Node localization attacks and Time Synchronization attacks. Many schemes were proposed by the researchers to protect sensor network from such attacks. Some of them are secure routing schemes[28] were proposed to control routing attacks, Secure Data aggregation protocols for Data aggregation, authentication schemes were used to eradicate false data injection attack

Revised Manuscript Received on May 07, 2019.

N.S.Usha, Research Scholar, St. Peter's University

Associate Professor, Department of CSE, S.A.Engineering College, Chennai, India

E.A.Mary Anita, Professor, Department of CSE, S.A.Engineering College, Chennai, India

and specific protocols were defined to defend localization and time synchronization attack.

The Layer-independent attacks are namely Node replication attacks, denial of service attack (DOS), Sybil attack, Signal or radio jamming attack, eavesdropping etc.

Many researches had proposed schemes that can detect the source of the attack but fail to be attacked resilient [29].Thus, there is a need for more effective schemes to identify the source of the attack and revoke them as early as possible to maintain the performance of the network.

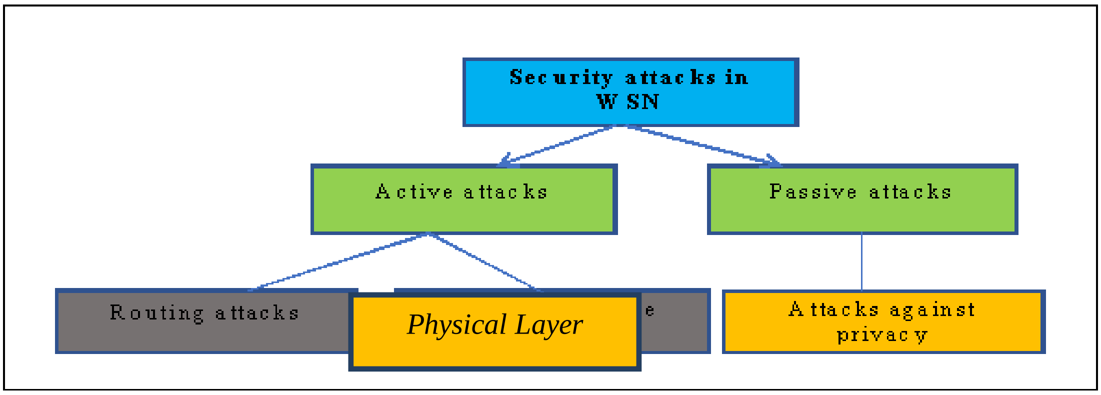


Fig. 1 Security attacks in WSN

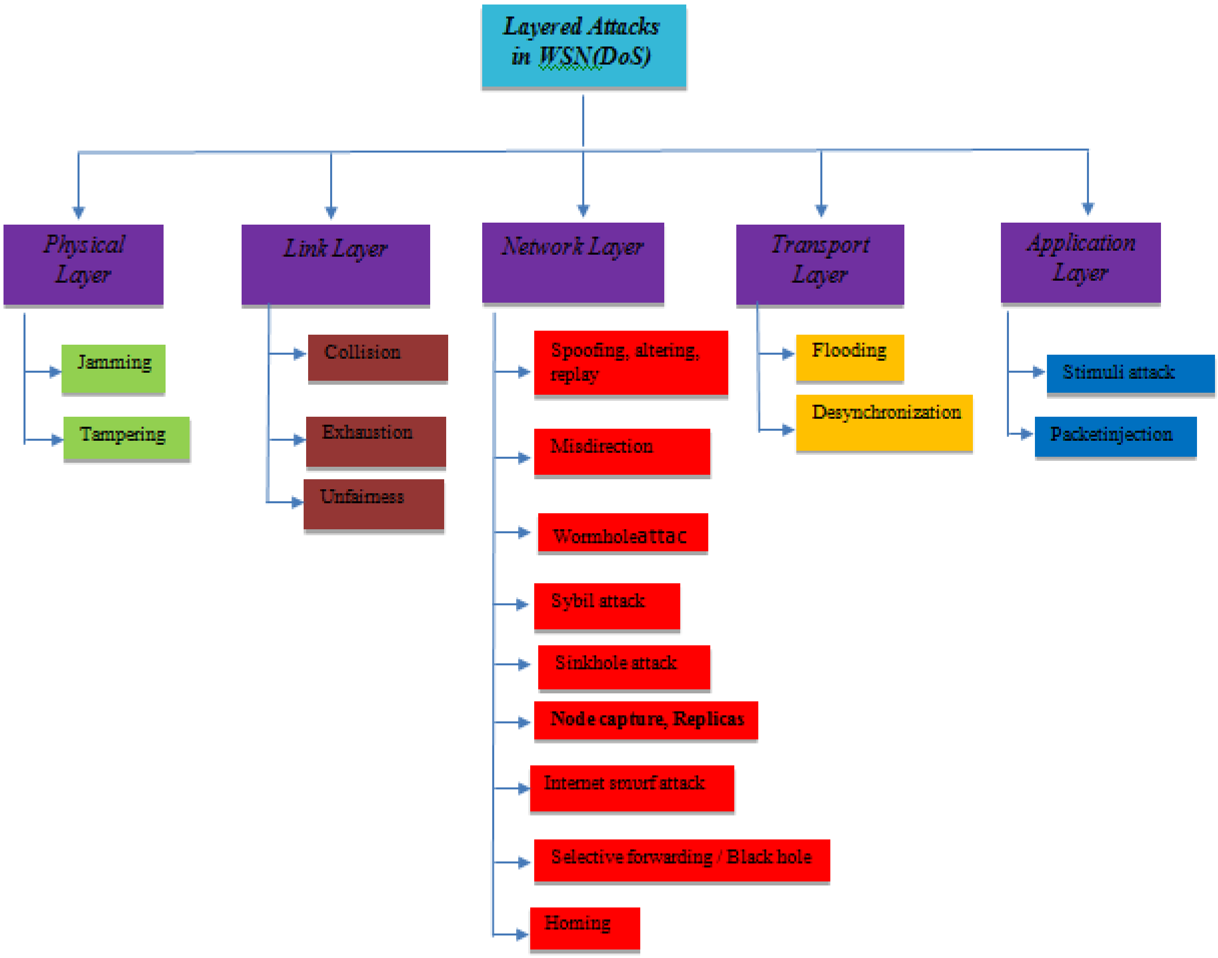


Fig. 2 Attacks in WSN

Node Replication attack

The presence of replicas or clones, disrupt the normal functioning of the network. Node replication attack mainly occurs when an adversary captures and compromises one node from the network. The adversary then copies all the essential details of the captured node, namely cryptographic information and secret credentials, using them creates one or more clones/replicas. The adversary makes these replicas accepted as legitimate nodes of the network and places them at strategic positions in the network to monitor and disrupt the network functionality. The adversary has the entire control over both the compromised node and the Clone node[5][7].

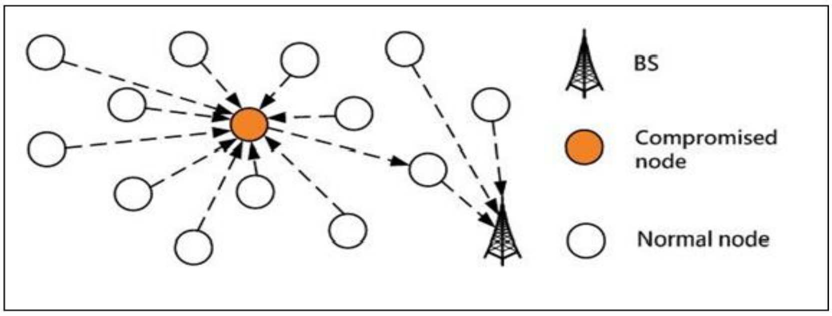
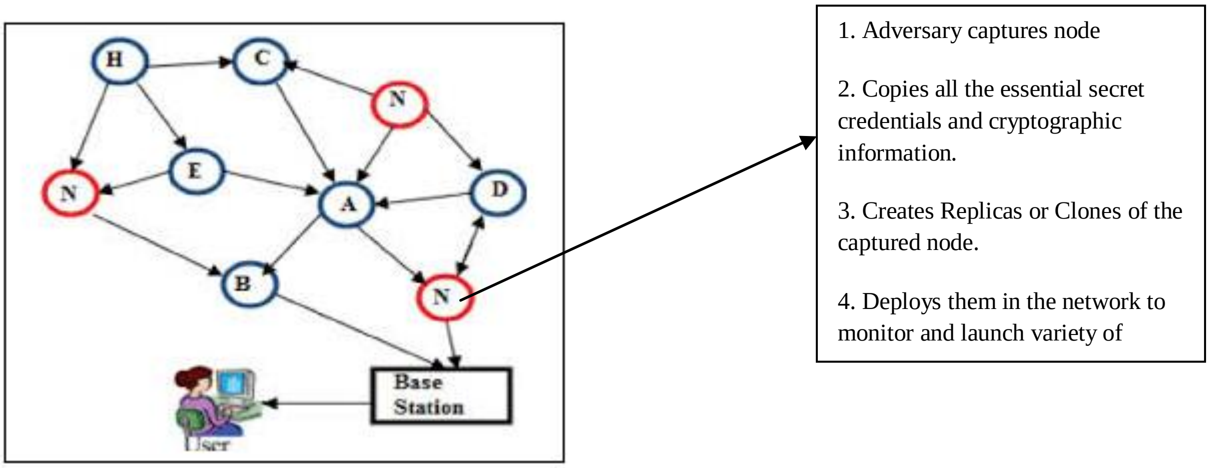


Fig. 3 Node Compromise by an attacker



1. Adversary captures node

2. Copies all the essential secret credentials and cryptographic information.

3. Creates Replicas or Clones of the captured node.

4. Deploys them in the network to monitor and launch variety of

Fig. 4 Scenario of Replication attack on nodes of WSN

Many researchers have proposed various detection schemes for the replication attack. However, most of the existing detection schemes cannot adapt to change in the network size and also they fail to revoke the network from attack within short span of time, thereby degrading its performance [21]. Mostly the detection schemes are classified into two main categories, namely Centralized and Distributed. Almost all the methods used in Distributed schemes are witness-claimer based or node-to-network broadcasting. These schemes depend upon a witness node for detecting clones in the network, suitable for the small network area. Also, these schemes fail to detect the presence of clones in multiple locations within a small period of time. Hence the centralized detection schemes are considered to be better in detecting replicas at multiple locations at the same time. The schemes are Base Station-based, Key-usage based, Cluster head-based, Neighbour-Social Signature based. All these schemes provide a high detection rate, but they suffer from a single point failure. In order to provide an efficient and quicker detection for Node replication attack, a new mechanism, namely BS-SECCISRNNA (Base Station based Secure Key Exchange Combined Clone Identification &Secure routing via Neighbour Node Authentication) has been proposed [14].

In this paper, an improvised Base Station scheme has been presented that provides simultaneous identification and safe routing of data to the destination. It does not suffer from a, single point failure, as the node is involved in Clone identification rather than the Base station.

The rest of the paper is organized as follows. Section II presents the related works, Section III defines the proposed model, and Section IV includes the proposed algorithm BS-SECCISRNNA. Section V provides the simulation results and its discussions. Finally the conclusion of the paper is given in Section VI.

II. RELATED WORKS IN CENTRALIZED DETECTION SCHEMES

Wireless Sensor Networks are mostly used in Battlefield Surveillance for secure transfer of commands between soldiers. As these nodes are deployed in large amounts in unattended environment they are prone to many attacks. One such major attack that causes security breach in the network is Node Replication attack. Replication attacks are mainly caused by an adversary, who captures one node in the network, copies all the cryptographic information and credential data, creates one or more clones of the captured node and places them at a strategic position in the network to monitor and disrupt the normal network functionality. The adversary makes these clones to be accepted as legitimate nodes by the existing nodes in the network[12]. Also the adversary has full control over both the compromised node and the clone node. Many Centralized detection schemes were proposed to detect the presence of replicas in the network. Normally the centralized schemes are classified into four types namely Base-Station based scheme, Key-usage based scheme, Cluster-Head based scheme and neighbour-Social Signature based scheme. Even though these schemes provided a proper detection procedure, but still they had many drawbacks.

Base Station based schemes

Centralized base station scheme

In 2004, the scheme proposed by Dutertre et.al is considered to be the most powerful scheme, where each node prepares a list of its neighbour nodes along with their location information and send it to the Base station. The Base station then scans the list and looks for same node ID's with two different locations (replicas). If node replicas were found, immediately the base station calls upon the revocation by flooding the entire network with the authenticated message. *This scheme delays the call for revocation as the Base station has to receive reports from all nodes in WSN and analyse them. As it suffers from single point failure, any compromise made on the BS may make the mechanism worthless [4].*

SET

In 2007, Cho. et al proposed a system that group's one hop neighbours into sub regions or sub trees and the details of it is sent to the Base Station. As the node ID's are unique, hence intersection of the sub regions or trees must be empty. The presence of intersection among the sub regions, confirms the existence of the clone or replica node in the network. This scheme has a high detection rate, but consumes more time and space when a large number of nodes were involved[10]. *It incurred high computation and communication cost, also due to its complex mechanism there is a possibility for adversary to use the revocation protocol to revoke honest or legitimate of the network.*

Sequential Probability Ratio Test (SPRT)

Ho et.al proposed a scheme in 2007 that determines the node capture attack in wireless sensor network. The captured sensor nodes are identified by sequential analysis mechanisms. This scheme makes use of the fact, that captured nodes may be unavailable during certain network operations, this information can be used for detection using a sequential probability ratio test. It calculates the absence time period of the node and checks it against the threshold value. If it proves to be higher than the threshold value, then that sensor node is declared as captured node. *This scheme mainly relies on the selection of threshold values for clone identification in the network [6].*

Space Time Related Pairwise key Predistribution Scheme (PSPP)

In 2007, the scheme proposed by Fei, et.al employs a polynomial for defining the key value of the node along with its installation time and location. In this scheme, Key value of the node is valid only within the deployed location. If the node leaves the location, the key value becomes invalid. This mechanism can be used to resist the network from clone nodes[9].

Active detection protocol

This scheme proposed by Melchor, actively identifies the presence of clone by involving each node to verify randomly few other nodes in the network. It does not construct any distributed database of location claims that searches for conflicting location to identify the clone. Here every node actively verifies nodes within 1km, and they send reports to BS. If two reports include conflicting location information for a node, then its declared as clone node[22]. *This scheme provides better detection rate, but still it cannot identify the presence of multiple clone at the same time in the network.*

Compressed Sensing based Clone identification (CSI)

In 2012, the technique proposed by Yu et.al, involves the nodes to broadcast a fixed sense data (β) to the one hop neighbours. The sensor nodes forward the (β) value to other nodes and finally the resultant value are aggregated by the BS. The BS then determines any node holding a value greater than (β) and declares it as clone nodes, as the legitimate nodes can forwards the value only once[13][30]. *Even though this technique possessed lower communication overhead, but still there is possibility of Single point failure, as the BS aggregates the values from all nodes and use it for identification of clones in the network.*

Neighbourhood Social Signature based schemes

Voting mechanism

In 2003,H. Chan, et.al initially proposed a Local Voting scheme, detect the replicas in the network. The scheme allows the neighbour nodes to cast public votes against the identified misbehaviour node[18]-[20]. If a node B sees that the public votes for a node A exceed the threshold t value, then B stops its communication with A. Eventually this scheme helped to identify replicas, but it is limited only to less number of neighbour nodes. *It failed to detect the replicas outside the neighbourhood. It also makes accuracy and sensitivity a challenging problem.*

Real time detection scheme

In 2008, the scheme proposed by Xing, allows each sensor node to compute a fingerprint value, using the neighbourhood information by applying a so-disjunct code. Each node stores the computed fingerprint value of its neighbours and attaches it with message for authentication at the time of transmission [15]-[17]. The clone nodes can be easily identified, as they show a mismatch in fingerprint, they also do not belong to the same community. Whenever the sensor nodes are deployed, they compute a fingerprint value for their community (social signature), which the clone node lacks even though they possess the same ID and keys as legitimate nodes but not the community value of the network. This specific property helps to identify the presence of clones in the network. Also the clones with different social or community signature can also be identified. *This scheme failed to handle new node entry or leaving the network. Also, there is a possibility of some clever clone nodes, to compute the community key and pass over the detection procedure.*

III. SYSTEM MODEL AND ASSUMPTIONS

This section presents two models namely the WSN Network model and the adversary model. A summary of all notations used are given in Table 1.

A. Network Model

A WSN network usually consists of a huge number of low-cost, light weight sensor nodes that are deployed in an unattended environment to sense or monitor environmental conditions such as pressure, temperature, humidity, soil fertility, heat, etc. As these nodes are very small, they are limited in sensing regions, possess less processing and computation power and they also depend on the battery power for the same. Normally the sensor nodes can directly communicate with one hop *ne* nodes called as their neighbour nodes[11].

Consider a WSN network consisting of *n* sensor nodes that are deployed over a region. The neighbour nodes of a node are identified by specifying the intensity range of 5 or 6 or 7. Likewise, each and every node identifies their nearest neighbour node and maintain the information in the table. A secret symmetric session key $K_s$is exchanged between the node and its neighbours that can be used for authentication.

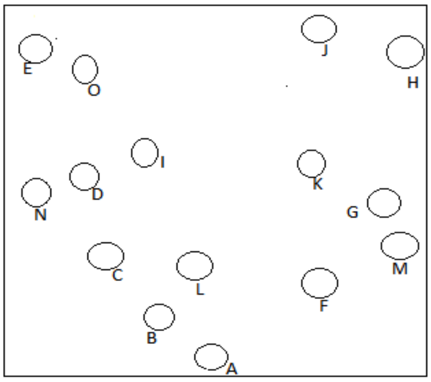


Fig. 5 Node deployment in Static WSN

B. Adversary model

An adversary captures one node from the network. Tries to copy all the credential details and cryptographic information's of the node and creates one or more clones/ replicas with same node ID, cryptographic materials, etc. The adversary then places these new clones/replica nodes at strategic positions in the network and try to hinder network functionality as it has full control over both the compromised node and the clone nodes. The adversary makes these clones accept as legitimate nodes of the existing nodes of the network, thereby avoiding the call of detection procedure [23]s. Using these replicas/ Clones the adversary can launch may insider attacks, thereby degrading the performance of the network.

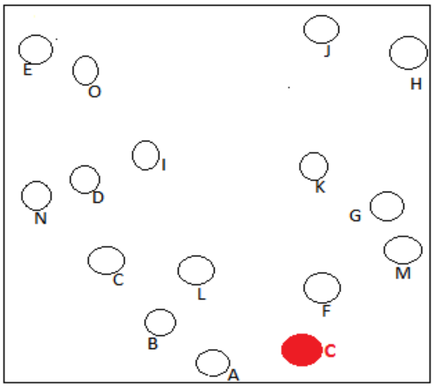


Fig. 6 Presence of Clone in the network

IV. PROPOSED SYSTEM

This section deals with the proposed system that simultaneously identifies the clone node and routes the data to the appropriate destination within a short span of time. The proposed system includes 6 main steps, namely, Network node initialization, Identification of Neighbour nodes, Route discovery, Secure Session Key Distribution Ks to Neighbour nodes, neighbour-neighbour authentication (Clone identification), Re-routing of Data to the desired destination.

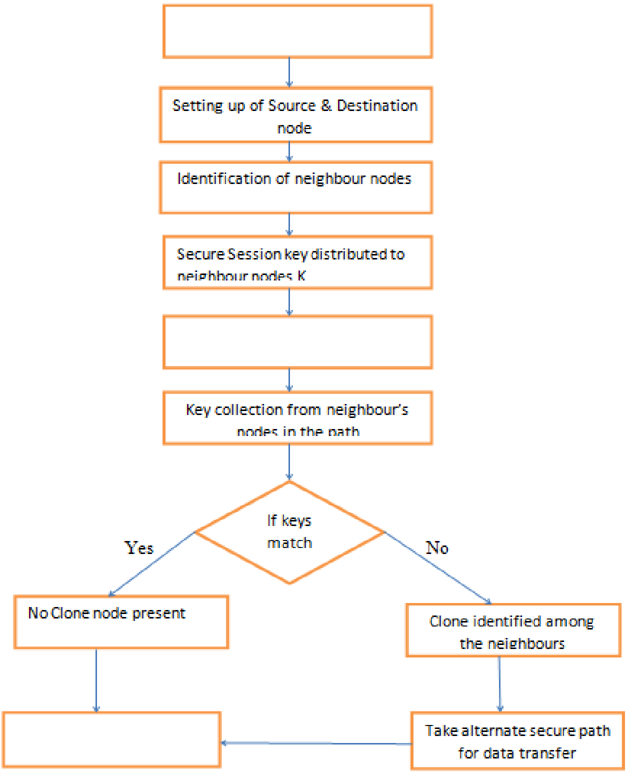

Setting up of Source & Destination node
Identification of neighbour nodes
Secure Session key distributed to neighbour nodes K
Key collection from neighbour's nodes in the path
If keys match
Yes
No
No Clone node present
Clone identified among the neighbours
Take alternate secure path for data transfer

Fig. 7 Flow Diagram of Clone Detection Process

[1] Network Initialization

Consider a WSN network consisting of *n* sensor nodes that are deployed over a region to monitor environmental conditions. The source and destination nodes are designed for secure flow of data between them. A secret symmetric session key *KS* is exchanged between the node and its neighbours that can be used for authentication as well as Clone identification.

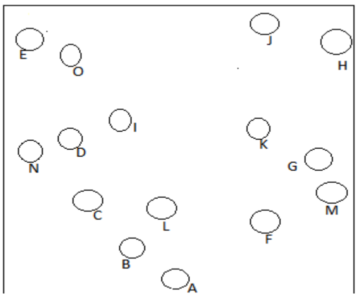


Fig. 8 Initial Node deployment in Static WSN

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

[2] Identification of Neighbour nodes

The neighbours of a node are identified by specifying the intensity value of 5 or 6 or 7. Likewise, each and every node identifies their nearest neighbour node and maintain the information in the table. The nearest neighbour is identified using radius-based neighbour learning algorithms, wherein the neighbours are identified based on some fixed intensity value. The distance between the neighbours is calculated using the Euclidean distance formula [27]. If the calculated distance is less than or equal to the given intensity value, then that particular node is marked as its neighbour node, else declared as not a neighbour of the node. The Euclidean distance between two points x and y is the line segment that connects them and it is given by

$$D(X, Y) = \sqrt{}\sum_{i=0}^{n} \quad (X_i - Y_i)$$

2

where X, Y are the Cartesian coordinates.

Algorithm- To find Nearest Neighbour node

```
Step 1. Let N= ($N_1$, $N_2$, $N_3$,….., Nn) be set of sensor nodes randomly deployed in the network.
Step 2. Set the range of the node R, to determine the Nearest Neighbour of a node.
Step 3. Compute the Euclidean distance between two points in the network, D(X,Y).
Step 4. If the computed value $D(X,Y) \leq R$, then node Y is neighbour of X.    Else
Step 5. The node Y, is considered to be out of range.
Step 6. Repeat steps 3 to step 6, to identify the nearest neighbours of each node.
Step 7. Finally each node maintains a table that contains nearest neighbour details.
```

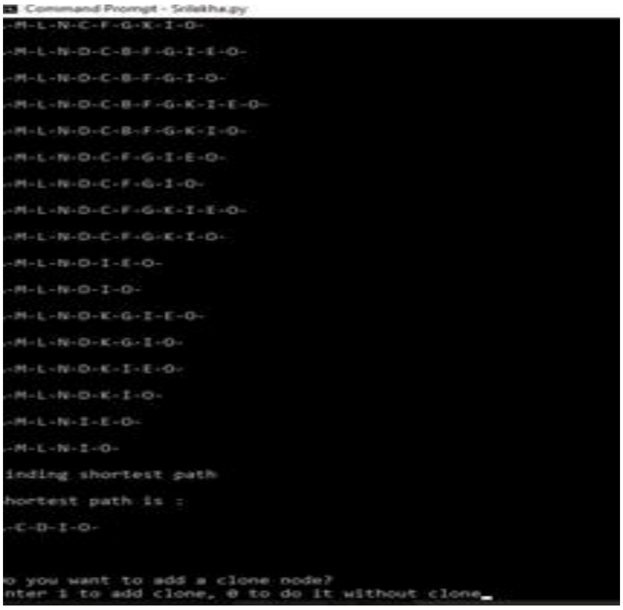
For a range value of 6, the neighbour nodes of Node A are given in the table.

Table. 1 Node-Neighbour details

Node	Next Hop
A	B
A	C
A	L
A	F
A	M

[3] Route Discovery

The Destination Sequenced Distance Vector algorithm (DSDV) is a table-driven or proactive routing algorithm defined for Wireless networks. This is an enhanced version of Bellman Ford algorithms, wherein each node maintains a table that contains the shortest distance to every other node in the network.. Every node stores the global topology information in the form of the table. The table gets updated whenever there is a path break or node failure. Also the nodes exchange their tables, if needed, for quick updating with respect to network topology. The routing table includes two main information, namely the node and its next hop. Based on the routing table information, the possible shortest paths from source node to destination node are identified. The shortest path chosen consists of the minimum hop count values. This routing algorithm offers less delay, as all the routes to destination is already available. The source and the designated node are defined, on applying the Dijkstra's shortest path algorithm, the possible routes between source and destination, as well as the shortest path between the nodes are displayed.



```
-M-L-N-C-F-G-K-I-O-
-M-L-N-D-C-B-F-G-I-E-O-
-M-L-N-D-C-B-F-G-I-O-
-M-L-N-D-C-B-F-G-K-I-E-O-
-M-L-N-D-C-B-F-G-K-I-O-
-M-L-N-D-C-F-G-I-E-O-
-M-L-N-D-C-F-G-I-O-
-M-L-N-D-C-F-G-K-I-E-O-
-M-L-N-D-C-F-G-K-I-O-
-M-L-N-D-I-E-O-
-M-L-N-D-I-O-
-M-L-N-D-K-G-I-E-O-
-M-L-N-D-K-G-I-O-
-M-L-N-D-K-I-E-O-
-M-L-N-D-K-I-O-
-M-L-N-I-E-O-
-M-L-N-I-O-
inding shortest path
hortest path is :
-C-D-I-O-


o you want to add a clone node?
nter 1 to add clone, 0 to do it without clone_
```

[5]Secure Session Key Distribution KS to Neighbour nodes

Once the shortest path between the Source and Destination are identified, the source node distributes a secret session is key to its nearest neighbour using the Nearest-neighbour table information. The session key KS is encrypted using BASE64 Encryption algorithms.

Let the shortest path between node A $\Rightarrow$ O be A$\Rightarrow$ B$\Rightarrow$C$\Rightarrow$D$\Rightarrow$ I$\Rightarrow$ O

Initially the source node A distributes the key to its nearest neighbour B, then from B to C, from node C to D, from node D to me and finally the node I distributes to its desired destination node O. The session key is distributed before every new data transmission between the source and destination nodes.

The session keyy is distributed as {E KS_s], T_s} from A to B. Likewise the nodes along the shortest path forward the key to nearest neighbour nodes in the path.

[6]Neighbour-neighbour authentication(Clone Detection)

The source node collects the key distributed to its neighbours [24]. On collecting the encrypted session key K_s, the source node applies an appropriate decryption algorithm and gets the key value. If it's able to decrypt the message, then is considered as honest neighbour, is designated as a Clone node.

Immediately all the nodes in the network update their neighbour table with new paths, excluding the clone node[26].

Algorithm- to find the Clone nodes in the network

Step 1. Let N=(A,B,C,D,E,F,G,H,I J,K L,M,N,O) set of sensor nodes deployed in the network.

Step 2. Let the range of intensity be R=6.

3. Each node identifies its nearest neighbour by calculating the Eucledian distance between them.

4. The source node and destination node are identified.

5. The shortest path from source to destination are identified using the nearest neighbour table of the node.

6. The source node distributes the session key K_s secretly to its nearest neighbour , neighbour- neighbour distribution takes places, until the key reaches the destination.

7. Before start of data transmission, the source node request it neighbour for the session key.

8. On applying the corresponding Decryption algorithm, the source node determines the key, also the node is designated as Honest node.

9. If decryption fails, then the node is identified as Clone node.

$A \rightarrow D[E[K_s]]$ = success, Honest node,

$A \rightarrow D[E[K_s]]$= unable to decrypt, designated as Clone node

[7]Re-routing of Data

If the designated, shortest path identifies a clone node, the source node with the help of its neighbour node, update the tables, as well as looks for the next shortest path in the network for secure transmission of the data[25].

Security Requirements

[1]Authentication

It is the process of validating a node before it can involve in the transmission of data to desired destination. It is carried out by distributing secret session key K_s to the participating nodes and later verifying the same at the time of data transmission. This mechanism mainly aids in identifying the presence of clones in the network, also helps in choosing an alternative path to reach the destination.

Step 1: The source node distributes the session key K_s secretly to its nearest neighbour , neighbour- neighbour distribution takes places, until the key reaches the destination.

Step 2: Before start of data transmission, the source node request it neighbour for the session key.

Step 3: On applying the corresponding Decryption algorithm, the source node obtains the key and the node is designated as **honest node.**

Step 4: If decryption fails, then the node is identified as **Clone node.**

$A \rightarrow D[E[K_s]]$ = success, Honest node,

$A \rightarrow D[E[K_s]]$= unable to decrypt, designated as Clone node

Step 5: The Time value T_S, mainly helps to identify whether it's a fresh message or old message.

[2]Data Integrity

Data integrity means, the transmitted data has not been altered or modified and reaches the destination safely. It mainly speaks about the validity of the transmitted data over time. Here the data is transmitted over a secure path that is free from clone/replica node.

Resilient to attacks

Sybil attack

Sybil attack usually poses a huge threat to Data Integrity. In Sybil attack, a single node forges itself and creates multiple copies of it, positions at various locations in the network and also makes the neighbour nodes accept them as legitimate nodes. By using the neighbour list, the presence of Sybil node can be identified, as the chances of commonality of neighbour nodes for Sybil node is always less. Also by the rule, a node can be neighbour to atmost 2-3 nodes only.

Replay attack

This is a network form attack. In Replay attack, the attacker/ hacker tries to eavesdrop the network communication, intercepts them, delays the data transmission or sometimes mislead the receiver to their commands. Here the network is safe from replay attack because of neighbour-neighbour authentication.

Black hole attack

In this type of attack, a malicious node, advertises itself as the shortest path to destination, thereby attracts all packets from source node to pass through it. As the source starts sending packet via the route, the attacker node drops it without forwarding it. This is termed as a Black hole attack. Here as the nodes undergo neighbour- neighbour authentication, the presence of black hole attacks is ruled out of the network.

Performance Analysis

In this section, simulation results are shown to evaluate performance of the algorithm BN-NACND (Base station based Nearest Neighbour Authentication Clone Detection algorithm) in identifying the presence of Replicas or Clones in Static Wireless sensor network. Here the simulation was carried out in python, with a network consisting of 15 nodes. Finally a graph has been plotted to show the difference in performance of the network, with / without clone.

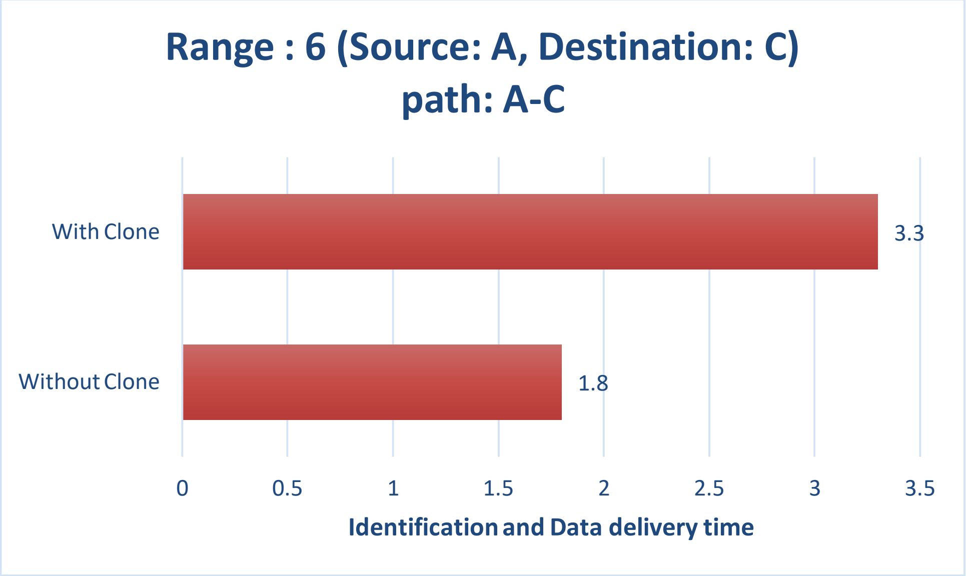


Fig. 9 Identification and Time delay in packet delivery with/ without Clone in the network with the source node range as 6

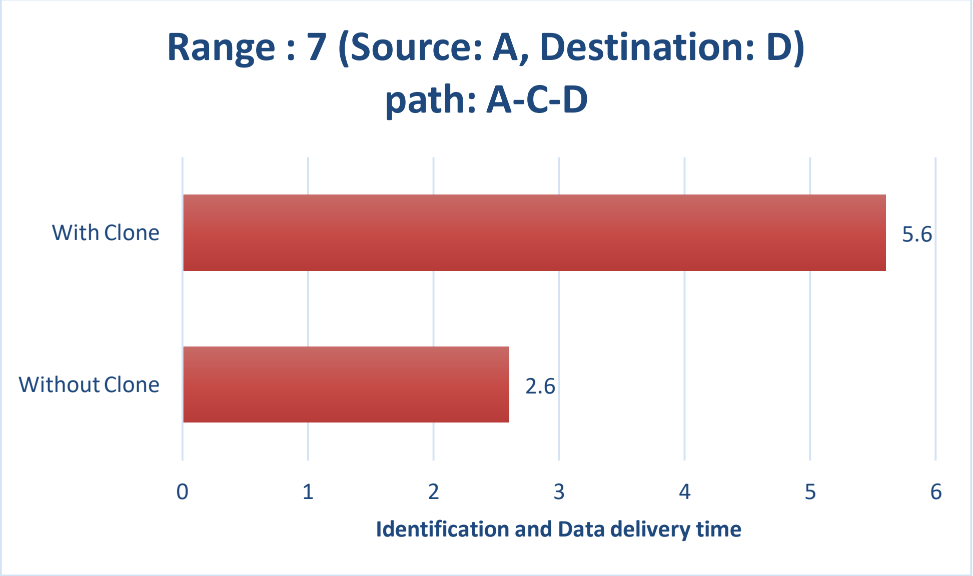


Fig. 10 Identification and Time delay in packet delivery with/ without Clone in the network with the source node range as 7

From the above graphs, it is clearly seen that as the range/ intensity of neighbour formation increases the time delay in packet delivery also increases. However, this algorithm BN-NCND can determine the presence of the clone at multiple positions at the same time in the network. Also, it offers 100% detection of clones and supports secure transmission of data through alternate paths even under the presence of Clone.

V. CONCLUSION

The proposed mechanism, BN-NACND (Base station based Nearest Neighbour Authentication Clone Detection algorithm) proved better in identifying the presence of Replicas or Clones in Static Wireless sensor network within short duration of time and also devised an immediate alternate path for the secure data transfer. It also helped in analysis of packet delivery ratio of nodes involved in transmission. The algorithm had a slight increase in time taken to deliver the packets with the presence of replica network of packet delivery.

REFERENCES

1. C. Karlof and D. Wagner,"Secure routing in wireless sensor networks: attacks and countermeasures", *in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.*
2. Haowen Chanand AdrianPerrig,"*Security and Privacy in Sensor Network", Carnegie Mellon University, October 2003*
3. HaowenChan, AdrianPerrig and Dawn Song ,Carnegie Mellon University,"Random Key PredistrbutionSceheme Key for sensor Networks", *2003.*
4. 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 (IEES and P'05), pp.49-63, May 2005.*

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

5. Carl Hartung, James Balasalle, Richard Han,”Node Compromise in Sensor Networks: The Need for Secure Systems*”, Technical Report CU-CS-990-05, Department of Computer Science, University of Colorado at Boulder, Jan 2005.*
6. H.Luo, L.Zhang,” Statistical en-route filtering of injected false data in sensor network*”,in Proceedings of the IEEE Journal on Selected areas in Communications, Vol. 23, No. 4, April 2005.*
7. Yun Zhou, Yanchao Zhang, YuguangFang,”Access control in wireless sensor networks”, *Elsevier 2006.*
8. Stallings, W,” Cryptography and network security: Principles and practices”, *(pp. 290–300) Pearson Education India, Delhi,2006.*
9. Fu, F., Liu, J., & Yin, X,”Space-time related pairwise key predistribution scheme for wirelesssensor networks*” in International conference on wireless communications, networking and mobilecomputing, 2007.*
10. Choi, H., Zhu, S., & La Porta, T. F, “SET: Detecting node clones in sensor networks”,*in Thirdinternational conference on security and privacy in communications networks and the workshops, 2007.*
11. Zhu, B., Addada, V. G. K., Setia, S., Jajodia, S., & Roy, S,”Efficient distributed detection ofnode replication attacks in sensor networks”, *in Twenty-third annual computer security applications conference, 2007, ACSAC 2007 (pp. 257–267), IEEE.*
12. Sohraby, K., Minoli, D., &Znati, T, ”Wireless Sensor Networks: Technology, Protocols, and applications (pp. 202–220)”, *Hoboken: Wiley,2007.*
13. Brooks, R., Govindaraju, P. Y., Pirretti, M., Vijaykrishnan, N., &Kandemir, M. T,”On the Detection of Clones in sensor networks using random key predistribution”, *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 37(6), 1246–1258,2007.*
14. Conti, M., Pietro, R. D., Mancini, L. V., & Mei, A,”A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks”, *in Proceedings of the 8th ACM international symposium on mobile ad hoc networking and computing, MobiHoc’07 (pp.80–89). Montreal, Canada: ACM, 2007.*
15. C.Bekara, M. Laurent-Maknavicius ,”A new protocol for securing wireless sensor networks against nodes replication attacks**”,***in Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2007*.
16. Y. Wei, Z. Yu, and Y. Guan, “Location verification algorithms for wireless sensor networks,” in *Proc. Int. Conf. Distrib. Comput. Syst.*, 2007, pp. 70–77.
17. K. Xing, F. Liu, X. Cheng, D. H.C. Du, ”Real-time detection of clone attacks in wireless sensor networks**,”** *Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS), 2008.*
18. Ko, L. C., Chen, H. Y., & Lin, G. R,”A neighbour-based detection scheme for wireless sensornetworks against node replication attacks”, *in Proceedings of international conference on Ultra-ModernTelecommunications and Workshops, ICUMT’09 (pp. 1–6). St. Petersburg: IEEE,2009*
19. Jun-Won Ho∗, Donggang Liu, Matthew Wright, Sajal K. Das*,*”Distributed Detection of Replicas with DeploymentKnowledge in Wireless Sensor Networks *“,Elsevier March 2009.*
20. Chano, SeungjaeShin, Chanil Park, Hyusoo Yoon , “A resilient and Efficient Replication Attack Detection Scheme for Wireless Sensor Networks*“,in IEICE Trans INE & SYST,Vol E92-D, No.7, July 2009.*
21. Roberto Di Pietro, Luigi V. Mancini, Claudio Soriente, Angelo Spognardi, and Gene Tsudik, “Data Security in Unattended Wireless Sensor *Networks*”,*IEEE TRANSACTIONS on COMPUTERS, Vol. 58, No. 11, November 2009.*
22. Wei Ding,BireswarLaha, Sumanth Yenduri,” First Stage Detection of Compromised Nodes in Sensor Networks”, *IEEE, 2009.*
23. B. Zhu, S. Setia, S. Jajodia, S. Roy, and L.Wang,” *Localized multicast:efficient and distributed replica detection in large-scale sensor networks”, IEEE Transactions on Mobile Computing, Vol. 9, no. 7, pp. 913–926, 2010.*
24. Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, “Random-walk based approach to detect clone attacks in wireless sensor networks,” *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 677–691, Jun. 2010.
25. Wenjun Gu, Neelanjana Dutta, Sriram Chellappan, and Xiaole Bai, “Providing End-to-End Secure Communications in Wireless Sensor Networks”,*IEEE Transactions On Network And Service Management, Vol. 8, No. 3, September 2011.*
26. Deng XM, Xiong Y,”A new protocol for the detection of node replication attacks in mobile wireless sensor networks*”, Journal of Computer Science And Technology 26(4): 732{743 July 2011. DOI 10.1007/s11390-011-1172-1*
27. G. Wang and K. Yang, “A new approach to sensor node localization using RSS measurements in wireless sensor networks,” *IEEE Transaction on Wireless Communication*, Vol. 10, no. 5, pp. 1389–1395, May 2011.
28. Wazir Zada Khan, Mohammed Y. Aalsalem,MohammedNaufal Bin Mohammed Saad, and Yang Xiang,”*Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey*”, *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 149023, 22 pages http://dx.doi.org/10.1155/2013/149023*.
29. K. Zhang, X. Liang, R. Lu, and X. Shen, “Sybil attacks and their defenses in the Internet of Things,” *IEEE Internet Things J., vol. 1, no. 5, pp. 372–383, Oct. 2014.*
30. Chia-Mu Yu, Chun-Shien Lu, Sy-Yen Kuo, “Compressed Sensing-Based Clone Identificationin Sensor Networks “,*IEEE Transactions On Wireless Communications, Vol. 15, No. 4, April 2016.*

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication