Detecting Node Capture Attacks Using Node Co-Operation and Ensuring Secure Routing in MANETs

P.P.Joby, C. Lincy Magdaline, M.Lavanya

Abstract— The Mobile ad hoc networks (MANETs) are prone to many security issues due to its nature and behavior. Particularly the node capture attack is common in this type of a network. This paper proposes a technique to detect node capture using node co-operation between the neighbouring nodes within the network and prevents false node capture assumption of nodes. The penalty and reward values are used to calculate the possibility of node capture. Avoiding major involvement of malicious nodes in communication path, and with the help of threshold and average values the efficient path is identified for establishing communication link. Thus, this technique improves the security and performance of nodes in the network.

Index Terms— ALARM-Time out message, Fault Assumption-Detecting the fault node, Links-Connection between nodes, MANET-Mobile ad hoc Network, Paths-Routes between nodes of a Network, Penalty-Negative remark on a node, Reward-Positive remark on a node.

1 INTRODUCTION

The MANETs has many security issues when transmitting mes… …en estal… …et-work. Th… …of attacks; … …In this, a no… …nd it is rep… …as maliciou… …vi-ties with… …nce efficienc…

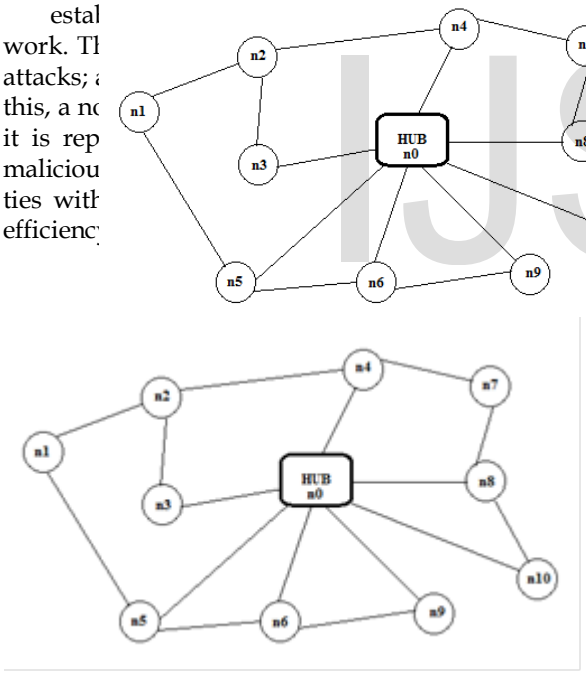

Fig 1.1- Simple MANET structure

- *Dr.P.P.Joby has completed his Ph.D.,in computer science and engineering under Anna University, India, E-mail: jobymone@gmail.com*
- *Lincy Magdaline.C is currently pursuing masters degree program in computer Science and engineering in PPG Institute of Technology under Anna University, India, E-mail:lincymagdaline@gmail.com*
- *Lavanya.M is currently pursuing masters degree program in computer science and engineering in PPG Institute of Technology under Anna University, India, E-mail:lavanyamarimuthu@gmail.com*

Considering the above simple mobile ad hoc network structure, let the source node be n1 and the destination node be n8. While establishing the communication link between source and sink, it involves multiple nodes in-between them. The intermediate nodes could be malicious nodes attacked by unauthorized users to perform malicious activities.

Thus to avoid malicious nodes within the network, there are many previously proposed solutions namely the key establishment, node re-meeting, etc., but they have few drawbacks like false node assumption i.e., false positive nodes and false negative nodes within the network. The false positive nodes are the nods present in the network which are detected and assumed to be a malicious node, but they are not actually malicious. The false negative nodes are the malicious nodes present in the network, but they are not detected and they perform malicious activities within the network.

In MANET all the nodes are mobile, so some nodes may be out of coverage and may be unable to communicate with other nodes. In such situation sometimes these nodes are assumed to be false positive node in the network. The false node assumption creates a major problem and it reduces the performance of the MANET. Thus, the node capture attack detection using local node cooperation concept is proposed in this paper to overcome the above mentioned backlogs in the network. Mobile Ad-Hoc Networks are a kind of Wireless Networks. Network topology often changes resulting in an unreliable network. If a node wants to connect to another node, the destination node must lie within the range of source node. They have the tendency to work deliberately free without any restrictions imposed on them.

MANETs possess the characteristics of free infrastructure which requires no ordered manner of implementation of packet transfer, the packets are not transmitted via a connection oriented route but is flooded so as to reach the destination packet, the network consists of nodes that have limited energy resource and hence require limited usage of energy, they are scalable so as to maintain any number of nodes. An issue to be

considered is the security of the network which is a hard task in a mobile network, as any node can enter the range and leave after the respected job is over. The trust of the network plays a highly important role in such network systems.

The MANETs include a few issues to be solved when being implemented, they are

Error Route:

Providing a good channel route that is not error prone helps to improve the efficiency of the network, and in case of presence of lags finding alternative paths for the packet to traverse.

Unknown Collidance:

When considered Nodes A,B and C, and node And C are in contact with C but not with each other, both tend to communicate with B resulting in colloidance. The solution for this problem is solved when each of the nodes ask for permission to send and receive packets.

When in case of exposed terminal, node D is only reachable from node Catha transmission of packets from node A to B would wrongly indicate that the node C is busy and hence delays the transmission from node D. this is a serious backlog as the transmission keeps delaying and the required data and the node suffers a incapability of transmitting packets and significant reduction of network throughput.

Limited Energy:

Nodes in MANETs rely on batteries or other diminishing sources of energy; hence the optimization of the network involves the energy conservation criteria. Maximum amount of energy gets wasted during the transmission and reception of packets. Many energy efficient concepts have been introduced among them the duty cycle concept conserves a significant amount of energy. This identifies the idle time of a node and reduces it by involving the node at intermediate cycles rather than continuous implementation.

Security Issues:

MANETs are more prone to security attacks, the proposed paper takes into account the issues such as the eavesdropping, spoofing, and denial-of-service for which efficient methodologies are being considered and avoids such security threats. A relationship is created between the sensor nodes which are done by a detecting mechanism which includes the penalty and reward points. These points help the assumption of a fault node and the path between the source and the destination.

The nodes that are assured to be the non-malicious nodes after the detection process are considered to be trust worthy and hence are allowed to use the resources while the malicious nodes are considered to be the unauthorized ones so the resources are blocked from these nodes. These malicious nodes are selfish nodes and are energy conservative and do not render back the services of help given by the network.

In the proposed paper, node cooperation concept is used, which involves the communication between neighbor nodes, thus prevents false positive node assumption within the network, the threshold value is set to identify the malicious node in the network, the penalty and reward values are calculated to each and every node present in the network. Thus, the average value is calculated for all possible communication paths. The best path is selected for establishing secured and efficient communication between sources and sinks in the network.

Section 2 describes about the previous related works in this field. Section 3 describes briefly about our new node cooperation concept. Section 4 contains simulated results and graphs. Section 5 concludes the paper, followed by references in section 6.

2 Comprehended Works

In MANETs, establishment of secured communication between source and destination nodes is a major problem. There are many previously proposed solutions for establishing secured communication without intervention of malicious nodes or unauthorized users within the network.

During early stages, key management concept was established in which each node is assigned with a specific key. The key is used to get access to the node and establishment of communication link with the node. The unauthorized users can't attack the node without the key, but if the key is broken, the network fails.

The concept of base station was proposed, in which all the nodes in the network are linked to the base station. If a node is not in communication with base station, then that node is assumed to be captured and attacked by unauthorized users, but it leads to false node assumption. It is impossible for a node to be in continuous communication with the base station, because the nodes are mobile in MANETs which leads to fault node assumptions. They are more widely used in fields such as the traffic monitoring, military, pollution monitoring and aspects of surveillances.

The concept of node re-meeting was proposed; in this all nodes present in the network are in constant communication with the base station within a time period. If the node does not come within the communication range of the base station, and if the base station does not receive any message from the node about its presence, within the time period then that node is assumed to be captured. Then the base station sends the information to all other nodes in the network, that the particular node is captured, so the node is not included for any further communication by other nodes in the network.

The nodes may have been in the intermediate process of communication with other nodes, or it might have been in transmission process which makes it unable to re-meet or respond to the base station. In such situation, the node might falsely be assumed to be captured and the node is revoked from the network. This reduces the performance efficiency of the network.

The US Defense Advanced Research Projects Agency (DARPA) developed the LANdroids, which are smart robotic nodes for battlefields. They are implemented in an unlikely environment for sharing information to soldiers which are really important and helpful; they also retain information for a long period of time. If there is a node capture by compromising its key, the result is disastrous. The solution to the problem is to solve the problems such as detecting the node capture as early as possible, to have a low rate of false assumptions and to have only a negligible amount of overhead.

Thus, the previously proposed solutions have few drawbacks. The proposed solution concentrates on overcoming the drawbacks of previous solutions. It concentrates on

detecting node capture as early as possible, it concentrates on avoiding false node capture assumption within the network to improve performance efficiency and it concentrates on finding energy efficient, secured communication path within the network.

3 NODE CO-OPERATION CONCEPT

Non cooperation of nodes result in pwer saving, this even when it sounds good has a major disadvantage of network availability. Node Cooperationis thus important to be implemented. MANETs differ from other networks as the nodes are not fixed and move around without a specific topology. They have a limited resoure such as energy, bandwidth and they cannot be trusted as there is no main authority.

Node cooperation is an essential element of a mobile network, as the nodes involved can act as a selfish node in case of emergency and no one has the authority to retrieve it back to its position or to maintain the complete network. For such situations the nodes contact each other and share about other nodes' positive and negative points which helps maintain a less selfish and a trustworthy network.

It has few challenges as any node can join the network and leave at any time it is requested and the malicious nodes are hard to be found out. Selfish nodes do not wish to render back the help that they once received from the network. The intervention of malicious nodes can be sorted out as a two way methodology, one is to punish the malicious node and the either option is to accept the network as it is. The reward points depicts how well the node behaves and how well it can be incorporated into a network. It helps us to come to a decision regrding the transmission of packets whether to trust the node are not to trust. This information is shared among the other node in the network so as to increase the networkreliability.

There are tpess of MANETs such as the VANETs which is Vehicular adhoc networks which tend to communicate the vehicle to the nearby equipment and helps when there is a collision of vehicles or any such undsirable sequence. The next one is the SPANs which are smart phone ad hoc networks which created peer-to-peer networks which creates a reliable mde of transmission even when there is a failure of a single node. The next type is the iMANETs which are internet based mobile ad hoc networks that connect to the fixed internet gateways, and the military or tactical MANETs that are indulged in military services such as security, range and information about the intervention of enemy troops.

One method to implement the node cooperation without the intervention of malicious attack is through the election of cluster head which sends information from its members in the network to the base staion and vice versa.

The nodes in thenetwork group together basedon the energy of the nodes and their identity is to be registered to the base station of the particular network. When an information is requested, it has to be unicasted by the base station to the cluster head and from the cluster head to the members. The cluster head is elected by the members in the network and hence there caanot be intervention of malicius nodes.

Reward points to a node are determined by direct observation of the node behaviour and the information of the good node is also being updated by other members in the network. Based on these different types of evaluation, the node average is found and through a series of the indulgance of the node the reward points are rendered. In this same manner the penaly points are rendered to nodes that are often being attackd or which does not produce a reliable outcome after a series of execution of packet transmissions from the source to the destination.

Flooding of requests can be handled by introducing a session key within which the requests can be sent and after expiration is cannot contact the nodes. This involves the key transmission which keeps changing ater a specific time period. In node co-operation concept, the perfomance of each node in the network is important to detect node capture and ensures secure routing within the MANET. This concept involves the inclusion of specific positive and negative values to each node in the network, namely the Reward and Penalty.

The proposed system contains the capture of nodes that have been accepted to be a trusted node, but have suddenly changed its tendency to become the attacker. Double mapping technique is used for such situation where the first mapping is done for the efficiency of the nodes and its trust to be authenticated by the neighbouring nodes. The second mapping is used to find the tendency of behaviour of the node at its next move. This is calculated using a constant value appended with the first map value and finally producing a predictable action that would be taking place at the next move of the node. The constant value changes according to the situation it is being implemented. This technique helps in identifying the attack of a trusted node, which proves to bring out a reliable network.

The above mentioned technique also is useful when the node is falsely being accused to be the attcker. The previous solutions implement the time period strategy within which the node has to contact the base station. When this fails it is determined to be the attacker, which may or maynot be true. The change in a nodes' behaviour is definitely a root reason for the occurence of an attack but there also might be situations where the node has a delay in packet transmission or a energy decrement during a transfer. This problem is sorted out using the calculation of average number of times the node fails and the averge number of times it has been successful. When the rate of failure being the highest it is considered to be an attacker while the rate bieng less is accepted to be trusted node. This data is being maintained for each node in the network.

The proposed system used the algorithm which clculates the reward value and finds each nodes goodness probability. This ensures that the packet is transmistted via a best path between the source and the destination. This makes the netwrok consistent and is highly reliable for a real time system that uses it. The MANETs being more prone to attacks need a high repulsion to error prone nodes and must use the nodes information accurately so as to avoid iterations over selecting the best path for the transmission of packets. The mechanism mentioned in the paper is scalavbe so as to accompany any number o nodes and are nearly accurate over

the selection of the best route for packet tranmission providing a minimum overhead on the network.

This system of working reqiures a prediction based environment which decides the nodes' goodness value based on the previous behaviour of the node. For a prediction to occur te attac must have been implemented in the network, which when after the attack the attacker can be determined by comparing the previous behaviur and th present behaviour. This leads to more number of resources to be used in the network. The threshold value has a constant appended to the maximum number of neighbours a node has.

When paths are selected for the transmission of packets, the respected paths' node value is calculated by the reward and penalty of the respected nodes and the average of this is calculated and the best among the paths is selected which has a relatively high goodness value and the packets are transmitted. This helps in easy evaluation of routing for the transmission of packets when compared to the early specified solutions. The base station holds the value of reward and penalty. An example of such reward and penalty values are presented in this table.

TABLE 1
PENALTY AND REWARD EARNED BY NODES

NODES	PENALTY	REWARD
n0	-	-
n1	5	5
n2	4	6
n3	7	3
n4	6	4
n5	1	9
n6	3	7
n7	2	8
n8	1	9
n9	7	3
n10	6	4

In Table 1, the nodes in the network are assigned with penalty points when they miss any transaction in the network through that node, and they are assigned with reward points when they complete a entire transaction without any retransmission or loss of packets.

The penalty and reward points are used to detect the node capture as soon as possible within the network. A threshold value limit(Tv) is assigned initialy in the network. When an node(i) in the network is not in communication with base station for a period of time, then an alarm message is sent, the threshold value(Ti) for that particular node is calculated and checks against the assigned threshold limit(Tv). If the calculated Ti is greater than value of Tv, then that node(i) has a possibility of being captured.

In this node co-operation concept, the false node capture assumption ratio can also be reduced, because in this before confirming that a node is to be captured and before there could be a flooding revoke message within the network, it sends an TimeOut(ALARM) message to the node and it checks for the exceedance of threshold limit of that node. Hence, the false node capture assumption is reduced and the performance of the network increases efficiently.

In this, the secured and efficient routing path is detected by calculating the path average with penalty and reward points of all nodes in the path, and the path containing maximum averge with high reward and low penalty is selected for transmission from source to destination within the network. Thus, this establishes an secure routing in MANETs.

If we consider a simple MANET shown in Fig 1.1 and if a communication link is to be established from node n1 to n8, then it may have many transmission paths within the network. For each path, the nodes are checked to ensure Is-not-Revoked and the average penalty and reward are calculated using the node co-operation algorithm, displayed in Table 2. The best path n1-n5-n0-n8 containing maximum path average, with low penalty and high reward are choosen for establishing communication link within the network with high efficiency.

TABLE 2
PATH AVERAGE PENALTY AND REWARD

PATHS	AVERAGE PENALTY	AVERAGE REWARDS
n1-n2-n3-n0-n8	4.25	5.75
n1-n2-n3-n0-n10-n8	5.66	4.33
n1-n2-n4-n7-n8	4	6
n1-n5-n6-n0-n8	3.75	6.25
n1-n5-n0-n8	3.66	6.33
n1-n5-n6-n9-n8	4	6

When traversing through the path n1-n5-n0-n8 the path has nodes that are considerably of higher path reward and less penalty gained leading to the highly efficient routing of packets from source to the destination. This is considered to be the path average from the different node values that were being implemented.

This system of mechanism involves the machine learning concept, in which the threshold value is already determined by the network itself. This concept is used to accept or reject a path based on the parameters mentioned. The packets are not sent as soon as the threshold value is reached. This is because the node stops communicating wen it reaches the threshold value limit. The path that has a node which has more penalty value has a less goodness value which turns the decision of path to a route with a high goodness value. This is an important criterion as the mobile node cannot predict the

attacker at the first time they are being included in the network.

3.1 Algorithm

Input-Network nodes(0-n), Source & Sink node
Output-Security routing path between source & sink
Source node → IDx;
Sink node → IDy;
Threshold value of each node →Tv;
Path_Avg=0;
Begin
TimeOut (Alarm);
for(i=0;(IsNeighbor(IDi,IDx)&(IDi<=IDy));)
{
if(Is-not-Revoked(IDi)
{
Ti = (Penalty(i)-Reward(i))/Total_No_Txn;
If(Ti<=Tv)
{
Update (Is-not-revoked(IDi));
else
flooding(Is revoked(IDi));
}
Avg(i)=Reward(i)-Penalty(i);
Path_Avg=Path_Avg + Avg(i);
}
If(IsMax(Path_Avg))
Nodes in Path_Avg →Path;
}
end

An alarm time out is to have a trigger at a specific constant amount of time and a revoke time out is to have an elapsed time out.

In Algorithm, the node co-operation concept is implemented between the nodes in the network. The source and sink nodes are assigned to IDx and IDy respectively. Then a threshold value limit(Tv) is declared.

Then to determine the communication path, it checks whether IsNeighbor(IDi,IDx) is true for node(i) within the network. And then it checks for Is-not-Revoked(IDi) and sends an Alarm message. The threshold value(Ti) is calculated using Penalty and Reward points of node(i). Then it checks for threshold exceedecce if(Ti <= Tv) is true and Update (Is-not-Revoked(IDi)), else if it is false, it detects the node to be captured and flood Is-Revoked(IDi) message to other nodes in the network.

Then the Path_Avg is calculated for node(i) if it is not revoked. Avg(i) is calculated using reward and penalty of node(i) and Path_Avg is calculated using Path_Avg = Path_Avg + Avg(i). From all possible paths, the path with maximum average is detected using IsMax(Path_Avg) and that path is selected for establishing secured transmission between source and sink nodes in the network without malicious nodes in it and with high performance efficiency.
The packet delivery ratio and overhead determine the network quality in which the packet delivery ratio is the ratio between the number of packets delivered to the number of packets to be actually sent. The availability of the network being the important issue is taken care of by the cluster head that manages the network providing better availability of network. Thus, the proposed concept detects node capture soon and avoids false node capture assumption and detects secured path for establishing communication in MANET.

4 Simulated Results

The proposed node co-operation concept is implemented using simulation tool and the output result efficiency is compared with previously proposed solution for node capture attacks in MANET.

The following graphs are the results obtained by simulating the node co-operation concept.

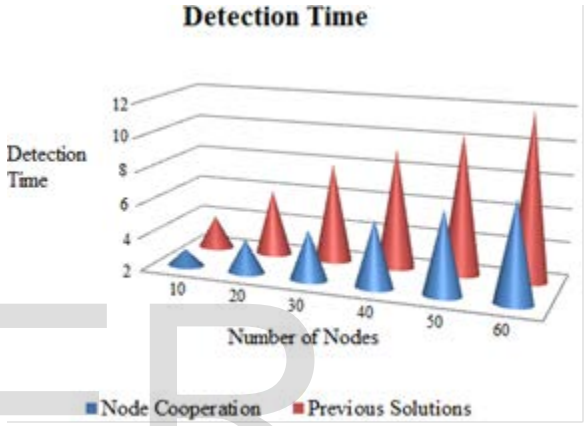

Fig 4.1- Node Capture Detection Time

The above graph indicates the results obtained by simulating the previously proposed technique and the proposed node co-operation concept with respect to node capture detection time period within the MANET.

The detection time involves a specific task of identifying node captures with respect to reward and penalty points. These points are then calculated for their average points when indulged as a path from source to sink. The graph thus indicates that the detection time period is comparatively reduced by implementing node co-operation concept in the network.

The fault assumption and the network performance are purely based on how the proposed system works and the output and result of how it is efficiently being implemented. The fault node assumption is nearly precise that it does not faulty assume the malicious nodes. The network performance of the proposed technique is considerably high that it completely uses the network availability for the betterment of the network.

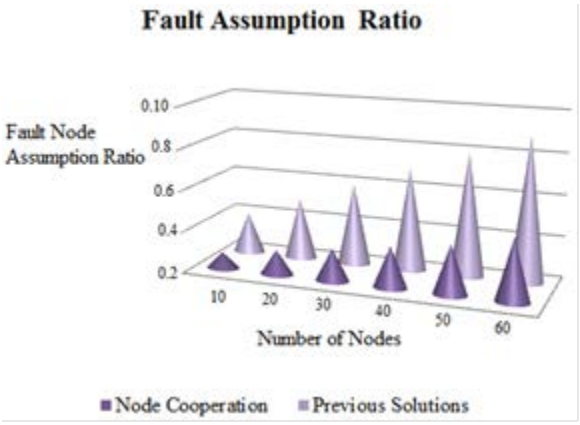

Fig 4.2-Fault Node Assumption Ratio

The above graph represents the fault node capture assumption ratio within the network. The implementation of node co-operation concept considerably reduces the fault node assumption ratio within the network, which reduces the intuition of good node as the malicious one and the malicious node to be a good one.

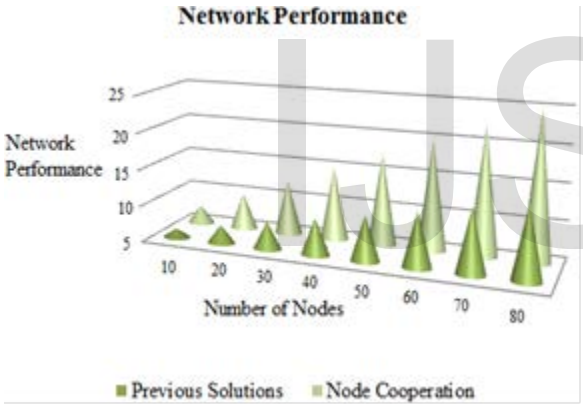

Fig 4.3-Network Performance

The above graph represents the network performance in MANET. The implementation of node co-operation concept considerably increases the performance efficiency of the network, by reducing the overhead in a network by implementing the algorithm for a selection of a best path among the available with less number of iterations for selection.

The above graphs indicate the result of node co-operation concept simulation and its improved performance in establishing secured communication within MANETs.

5 Conclusion

The major problem in communication establishment in MANET is detecting node capture attack. The proposed technique involves the node co-operation concept to overcome the problem with higher efficiency in detecting node capture compared to previously proposed solutions. The major requisition on ad hoc networks is the implementation of secured routing and another major challenge in MANETs are unreliable wireless connections. The proposed model provides robustness for the entire network system with a negligible amount of failure occurrence.

The future enhancement of this paper can be done related to performance of routing protocol in terms of Qos and calculating optimal paths minimizing the time consumption for calculating and confirming node capture thereby avoiding false node capture assumption within MANETs.

Acknowledgment

We would wish to thank Lord Almighty for helping us complete the paper, and we are greatful to the PPG Institutions for rendering us the support for completing the research paper.

References

[1] H. Chan, A. Perrig, and D. Song, "Randomkey predistribution schemes for sensor networks," in Proceedings of the IEEE Symposium on Security and Privacy (S&P '03), September 2003.

[2] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," in Proceedings of the 3rd International Conference on Information Processing in Sensor Networks (IPSN '04), April 2004.

[3] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '06), pp. 564–568, New York, NY, USA, June 2006.

[4] R.Di Pietro, L. V.Mancini, and A.Mei, "Energy efficient nodeto- node authentication and communication confidentiality in wireless sensor networks,"Wireless Networks, vol. 12, no. 6, pp. 709–721, 2006.

[5] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '07), pp. 80–89, 2007.

[6] B. Parno, A. Perrig, and V. D. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proceedings of the IEEE Symposium on Security and Privacy (S&P '05), 2005.

[7] Information Processing Technology Office (IPTO) Defense Advanced Research Projects Agency (DARPA), BAA 07-46 LANdroids Broad Agency Announcement, 2007, http://www.darpa.mil/index.html.

[8] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Commununications of ACM, vol. 47, no. 6, pp. 53–57, 2004.

[9] S. Capkun, J.-P. Hubaux, and L. Butty´an, "Mobility helps security in ad hoc networks," in Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '03), pp. 46–56, 2003.

[10] C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks," in Proceedings of the 2nd International Conference on Security and Privacy in Communication Networks (SecureComm '06), Baltimore, Md, USA, 2006.

[11] P.P. Joby , Sengottuvelan, " A Localised clustering scheme to detect attacks in wireless sensor Networks" International journal of electronic security and digital forensics, vol 7, No.3,2015.

[12] G. Sharma, R. Mazumdar, and N. B. Shroff, "Delay and capacity trade-offs in mobile ad hoc networks: a global perspective," in Proceedings of the 25th Conference on Computer Communications (INFOCOM '06), 2006.

[13] A. Becher, E. Becher, Z. Benenson, and M. Dornseif, "Tampering with

motes: real-world physical attacks on wireless sensor networks," in Proceeding of the 3rd International Conference on Security in Pervasive Computing (SPC '06), pp. 104–118, 2006.

[14] M. Grossglauser and M. Vetterli, "Locating nodes with EASE: last encounter routing in ad hoc networks through mobility diffusion," in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '03), San Francisco, Calif, USA, 2003.

[15] P.P.Joby, P.Sengottuvelan, "On the construction of virtual topology structure for secure routing in wireless sensor Networks", Sensor Letters Vol 13, 946-952, 2015.

[16] C. fanHsin and M. Liu, "A distributed monitoring mechanism for wireless sensor networks," in Proceedings of the Workshop on Wireless Security (WiSe '02), pp. 57–66, 2002.

[17] C. fan Hsin and M. Liu, "Self-monitoring of wireless sensor networks," Computer Communications, vol. 29, no. 4, pp. 462–476, 2006.

[18] N.Hayashibara, A. Cherif, and T. Katayama, "Failure detectors for large-scale distributed systems," in Proceedings of the 21st IEEE Symposium on Reliable Distributed Systems (SRDS '02), Suita, Japan, October 2002.

[19] M. Haibo, J. Peng, and J. Bigham, "Augment delay tolerant networking routing to extend wireless network coverage," in International Conference on Wireless Communications and Signal Processing (WCSP), Nov.2011, pp.1–5.

[20] W. Jianjian and W. Ronghui, "A routing algorithm based on energy constraint," in International Conference on Computer Research and Development (ICCRD), vol. 2, Mar. 2011, pp.330–332.