Asian Journal of Information Technology 15 (4): 808-816, 2016
ISSN: 1682-3915

Trust Based Collaborative Attack Detection in MANET

A. Jayanand and N. Chenthil Kumaran
Faculty of Computer Science and Engineering, Maria College of Engineering and Technology,
Attoor, Tamil Nadu, India

Abstract: The MANET faces critical issues due to the various attacks like wormhole, black hole, greyhole and even collaborative attacks. To overcome this issue, we propose to develop a detection scheme to detect and prevent collaborative attacks. Initially, clusters are formed with neighbourhood of nodes with a monitor node with all nodes at its 1 hop neighbours. This monitor node is chosen using an algorithm considering the willingness and trust value of a node. Then, we use ADCLU algorithm utilizing the monitor node to detect malicious nodes in a neighbourhood of nodes. Here, each pair of nodes may not be in radio range of each other but where there is a node among them which has all the other nodes in its 1 hop vicinity. The detection is based on voting from all other nodes about a certain message. The malicious node detected is isolated and further communication with this node is stopped.

Key words: Dedect, ADCLU algorithm, neighbourhood, 1 hop vicinity, India

INTRODUCTION

Mobile Ad hoc Network (MANET): The MANET is a multi-hop wireless network are composed of autonomous nodes that communicate with each other by forming dynamic topology such that nodes can easily join or leave the network at any time without any fixed infrastructure such as access points or base station and maintaining connections in a decentralized manner. The network over radio links are caused due to the self-organization of the mobile nodes. Each device in a MANET is free to move independently in any directions (Patel and Sharma, 2013). The infrastructure less property and the easy deployment along with the self-organizing nature makes them useful for many applications like military applications, mobile social networks, emergency deployment, intelligent transportation systems and fast response to disasters (Mathew and Petchimuthu, 2013).

The MANET also throws a security challenge due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points and lack of clear lines of defense moderate bandwidth, limited battery power, computational power and limited resources. So, mobile Ad-hoc networks are vulnerable to several different attacks (Singh *et al*., 2014).

Collaborative Attacks in MANET: The collaborative attacks are defined as two or more types of attacks such as the black hole attacks and the wormhole attacks which synchronized simultaneously in the network in a collaborative way (Gong and Bhargava, 2013). It is a synchronized attacks where a system is distributed by more than one attacker simultaneously or involving two or more colluding nodes that can be processed using wired or wireless link and triggered by single or multiple attackers. Collaborative Attacks (CA) occur when more than one attacker or running process synchronize their actions to disturb a target network but not necessarily in collaborationwhere every attack is launched by a specialized expertise. These attacks can be classified into two different categories (Dureja and Dahiya, 2014).

Direct collaborative attacks: Here, the attacker nodes are already in existence in the original network or a malicious node joins the network or an internal node is compromised in the network. This kind of collaborative attacks can be referred to as direct collaborative attacks. For examples, black hole and wormhole attack.

Indirect collaborative attacks: The attacks in this category use different non-existent nodes in order to fake other nodes to redirect data packets to malicious node.

Corresponding Author: A. Jayanand, Faculty of Computer Science and Engineering, Maria College of Engineering and Technology, Attoor, Tamil Nadu, India

This kind of collaborative attacks can be referred to as indirect collaborative attacks. For examples, sybil and routing table overflow attacks.

Collaborative attack detection in MANET: Collaborative attacks in ad hoc networks carriage challenges to the detection system. Malicious nodes may collude to conduct more complex and subtle attacks to prevent detection or identification. To detect against collaborative attacks essential that monitoring and detection agents collaborate efficiently. The collaboration should include each existing node in the network. The main challenges include:

- Integrating the information from multiple nodes in efficient manner
- For developing the attack detection mechanisms that should be robust against noise in the information
- For discovering the effective relationship between the range of network from which the information is integrated and the detection capabilities of the mechanisms
- Determining the trade-off between the detection granularity and the dynamics of the networks (Bhargava *et al*., 2009).

Literature review: Mathew and Petchimuthu (2013) have proposed a collaborative watchdog based on contact dissemination with a log file system. The watchdog has detected a selfish node in the network then spread the information to other nodes when contact occurs. The detection of the contacts among the nodes is performed based on the node's watchdog for the detecting the selfish nodes. Log file system have used for reducing the detection time of the selfish node. After forwarding, the packets from the neighbor node to next neighbour node, neighbor node could not overhear the packet dropping of next neighbor node either if transmission collides between source and neighbour node or neighbour node is not within the transmission range of next neighbour node. When this happens it could not provide the security.

Gong and Bhargava (2013) have proposed to defend the ad hoc network under collaborative attacks such as the black hole and the wormhole attacks using new tri-tier cooperative immunization from the inspiration of the human immune system. Tri-tier immunization includes native immune tier to recognize known attacks, adaptive immune tier to learn unknown attacks and parallel immune tier is built with the cloud-computing infrastructure for increasing both the efficiency and robustness of immune computation. The approach provides immunization to isolate the nodes under attacks by the network reconfiguration. Still it provides security reconfiguration is not possible.

Nouri *et al.* (2011) have proposed a collaborative technique for detecting a wormhole attack in that neighborhood using clustering. Monitor node initiates the detection process by passing messages between the nodes and depending on the messages received determine suspected nodes that sent to the monitor node. The suspected nodes receive at least a minimum number of votes or only one vote are finally detected as malicious nodes by inspecting the votes at monitor node and isolate malicious nodes from a group of nodes in routing process. But, using this technique is not possible for detecting wormhole attack in the form of out of band attack. When, there is congestion or collision, a node may be dropping packets due to overloaded and so the algorithm will not work properly. And also if a monitor node continuously monitoring the detection process, it may cause exhausting of battery power because of overhead of being the monitor node.

Chang *et al.* (2015) have proposed a Cooperative Bait Detection Scheme (CBDS) by designing a DSR based routing mechanism for detecting and preventing malicious nodes that attempts to launching gray hole/collaborative black hole attacks in MANETs that incorporates the advantages of both proactive and reactive response. Using a reverse tracing technique malicious nodes are detected and prevented from participating in the routing operation. When a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again and the dynamic threshold value can be adjusted according to the network performance. However, if a lower thr value is set, some of neighbors of the suspicious node may not be found.

Sen *et al.* (2007) have proposed a distributed protocol for detection of packet dropping attack based on cooperative participation of the nodes in a MANET. The protocol works through cooperation of some security components that are present in each node in the networks such as monitor, trust collector, trust manager, trust propagator and whistle blower by using complementary relationship between cryptographic key distribution and intrusion detection activity. The redundancies in routing information make the detection scheme highly robust and secure and using of controlled flooding technique has very low communication overhead. However, after finding

the malicious node it does not consider the technique for isolating the malicious node from participating in routing process.

Yu *et al.* (2007) have proposed a distributed and cooperative mechanism for detecting potential multiple black hole nodes through collection of some local information. From the information, nodes evaluate that there exists any suspicious node among their one-hop neighbors. After finding, the node as a suspicious, a cooperative procedure will be initiated to further check the potential black hole nodes. Then, the global reaction is initiated to form a proper notification system to send warnings to the whole network. However, overhearing for collection of local information does not work always properly in situation like collision or weak signal. It leads to incorrect evaluation of the behaviour of the suspicious node.

Wang *et al.* (2009) have developed a new mechanism for audit based detection of collaborative packet drop attacks using hash function based method to generate node behavioral proofs that contain information from both data traffic and forwarding paths. Intermediate node construct a bloom filter based on the contents of the packets to generate the behavioral proof. It allows the system to successfully locate the routing segment in which packet drop attacks are conducted. However, other nodes cannot find the difference between an audit packet and a common data packet. Security is based on the value of its behavioral proof. So, it is not efficient. If, there is no malicious node all packets are delivered to destination without any packet dropping at intermediate node. So, it does not analyse any scenario for delivery of packet ratio at destination.

Banerjee (2008) have proposed detection and removal of cooperative black and gray hole attack in MANETs. The total data traffic is divided into small blocks for ensuring an end-to-end checking. Before sending any block source sends a prelude message to the destination to aware the incoming block. Flow of the traffic is monitored by the neighbors of the each node. At the end of the transmission destination node sends postlude message containing the no of data packets received. Using this ack source node check whether the data loss is within the tolerable range, if not then the source node start the process of detecting and removing malicious node by collecting the response from the monitoring nodes. However, the ability of this algorithm is based on finding the threshold probability of non-malicious packet drop. If the threshold probability for non malicious packet drop is low, this algorithm identifies any malicious behaviour. But, also it means that increases the false detection rate.

Problem Identification: Nouri *et al.* (2011) proposed collaborative techniques for detecting wormhole attack in MANETs using the ADCLU algorithm (Algorithm for Detection in a CLUster). This algorithm can be performed with the cluster head as the monitor node using existing cluster. If a monitor node continuously monitoring the detection process, it may cause exhausting of battery power because of overhead of being the monitor node. Whether, there is a congestion or collision at any node, the node may be dropping of packets due to overload. Meanwhile this algorithm does not consider the reason for dropping of packets. Then, it finds the out of band wormhole attack based on threshold value. It is not efficient for providing security. When noticing all the nodes in the network for identification of occurrence of event sometime this algorithm is unsuccessful.

MATERIALS AND METHODS

Proposed solution: To overcome this issue, we propose to choose an efficient monitor node based on the willingness and trust value of a node. Hence, the monitor node could have the ability to continuously monitor the detection process without battery power exhaustion due to overhead problem. This administrator node can cover most of the 2-hop neighbour of its selector. In case of tie, node with higher trust/power will be selected. This monitor node can be used for detection of malicious nodes.

Overview: The MANET faces critical issues due to the various attacks like wormhole, black hole, grayhole and even collaborative attacks. To overcome this issue, we propose to develop a detection scheme to detect and prevent collaborative attacks. Initially, clusters are formed with neighbourhood of nodes with a monitor node with all nodes at its 1-hop neighbours. In the cluster, we choose a node as monitor node based on trust and willingness of a node. Based on these factors, an algorithm choose administrator node. This node can be used as monitor node in ADCLU algorithm to detect malicious nodes in a neighbourhood of nodes. Wherein, each pair of nodes may not be in radio range of each other but where there is a node among them which has all the other nodes in its one-hop vicinity. The detection is based on voting from all other nodes about a certain message (Fig. 1).

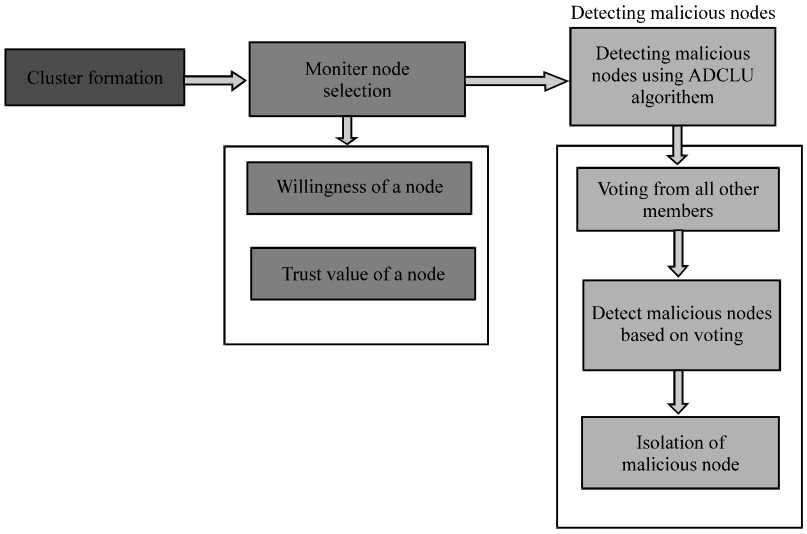

Fig. 1: Block diagram of the entire algorithm

Monitor node selection: Initially, a cluster is formed with a neighbourhood of nodes which consists of a node with all other nodes as its 1-hop neighbours. In the cluster, the monitor node is chosen based on willingness and trust value of a node considering the more exhaustive parameters and minimizes the admin node count. This mechanism encourage traversing the same path return while sending. The admin node can also switch from one node to another on extreme need, offloading its job to other node increasing runtime.

Willingness function: The willingness value is calculated with a weighted sum of node's battery power, coverage area and reliability of the node and cost of trusted opportunistic route. The MANET power factor is critical hence given highest weight value, etc. All weights are experimentally tested and optimized value for the scheme (Wang *et al*., 2009):

$$\text{Willingness}(Pw,Cv,R,CTR) = (0.5\times Pw) + (0.15\times Cv) + (0.1\times R) + (0.25\times CTR) \quad (1)$$

Where:

Pw = Available power for that node (%)
Cv = Coverage (%)
R = Reliability of node (%)
CTR = Cost of trusted opportunistic routing (%)

They are calculated as follows:

$$Pw = \left(\frac{\text{Current node power}}{\text{Rated nodel capacity}}/\right)100 \quad (2)$$

$$CV = \frac{\text{No. of 1 hop neighbors of that node}}{\text{No. of 2 hop neighbors of node which need to select this node as admin}}\times 100$$

$$CTR = \text{Cost of Trusted opportunitics} \quad (3)$$

The R is estimated from various sensor inputs regarding outside environment condition in which R ranges from 0-100% based o nodal positions:

$$R = \{0....100\%\} \quad (4)$$

Choosing admin node: An algorithm chooses the node which could cover most of the 2 hop neighbour of its selector as administrator node. This selection considers willingness and trust value of a node. The node with higher trust/power will be chosen in case of a tie. Before forming an algorithm, we assume:

- ad (a) → admin set of node a running the algorithm
- $Ns_1(a)$ → 1 hop neighbour set of node a (symmetric neighbours)
- $Ns_2(a)$ → 2-hop neighbour set of node a (symmetric neighbours of nodes in Ns (a)). The 2 hop neighbour set $Ns_2(a)$ of node a do not contain any 1-hop neighbour Ns (a) of node a
- d(a, b)→degree of 1 hop neighbour node b (such that be$Ns_1(a)$) is referred as the number of symmetric 1hop neighbours of node b without node a and all symmetric 1 hop neighbour of node a:

$$d(a,b) = Ns(b) - \{a\} - Ns(a) \quad (5)$$

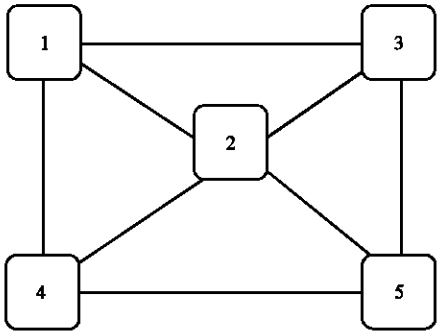

Fig. 2: Cluster with node which has all other nodes in its 1-hop neighbours

Where:

Wi = Current willingness of node ranging from 0-7

T = Trust value of node and has a range of 0-7 and trust threshold is application oriented

Admin node selection algorithm

Initialization: Initialize node trust table with default trust value 3 for each node and path list as []

Algorithm:

begin with empty admin set ad(a)={}
calculate d(a,b) where b is a member of $Ns_1(a)$ for all nodes in $Ns_1(a)$ (all +ve sign)
first choose admin node= nodes who provides $Ns_1(a)$ a single path to reach some of nodes in $Ns_2(a)$
for (each node in $Ns_1(a)$)
{
Choose admin node=current node as per Table 1
While if (some node still in $Ns_2(a)$ not covered by ad(a))
{
for each node in $Ns_1(a)$, Calculate no of nodes in $Ns_2(a)$ not yet covered by ad(a) and can be reached via 1-hop neighbour of a
}
Choose admin node=node of $Ns_1(a)$ which attain maximum no. of uncovered nodes in $Ns_2(a)$ and refer Table 1
In case of a tie, choose node with higher d(a,b) as admin node and refer Table 2.
}
process each node b in ad(a),one at a time for optimization.
If ad(a)-{b} still covers all nodes in $Ns_2(a)$
{
remove b from ad(a)
}
Then convert link between node a and ad as sym_link to admin_link
Exit

ADCLU algorithm: The chosen monitor node in a cluster is formed with a neighbourhood of nodes with all other nodes as its 1-hop neighbours. The ADCLU algorithm (Algorithm for Detection in a CLUster) detects malicious nodes in a set of nodes forming a cluster. Here the nodes may not within radio range of each other (Fig. 2).

Before presenting the algorithm, we make certain assumptions like wireless links between nodes are bi-directional. On monitor node initiating the detection process, malicious nodes will not be aware of the progressing algorithm as in case of ADCLI algorithm (Algorithm for Detection in a CLIque). Now ADCLU Intrusion Detection algorithm consists of following steps. Let M be the monitor node, N be the neighbour node of M, MVR be the malicious vote request message, m be the original message, WM be the wrong message:

- Initially, the monitor node M broadcasts the message m to its neighbour nodes requesting to further broadcast the message in their neighbourhood
- When message m is received by each neighbour N of monitor node M, N further broadcast message m in its neighbourhood
- The monitor node M then broadcasts a malicious-vote-request message MVR in its neighbourhood
- When malicious-vote-request message MVR is received from M, each neighbour N of M perform as follows

Let, node N receives message s from node A from step (ii). If node N neither receives any message from A or if it receives a message different from m, s is assigned default message WM (Wrong Message). If s = m, then N sends a vote for node A, being a suspected node to M:

- When votes are received, the monitor node accept only distinct votes from each node since distinct votes enable monitor node to accept at most one vote about a suspected node from any node
- Let, n be number of votes received for node A. If $n \geq j$ then node A is marked as malicious. (The monitor node also votes and j is threshold value)

Once, the wormhole attack is detected, the algorithm should disconnect, these malicious nodes from routing process and convey this to the other nodes in this cluster and especially monitor nodes in different clusters to not use them in routing process. The vital thing is the amount of threshold that the algorithm specifies for amount of j to detect wormhole attack (Fig. 3).

Special case: Suppose, two malicious nodes of wormhole attacks are in different clusters. An out-of-band high bandwidth channel launches this mode of wormhole attack. Other modes of wormhole attack use high power transmission or relaying packet between two distinct malicious nodes in different cluster or the same one.

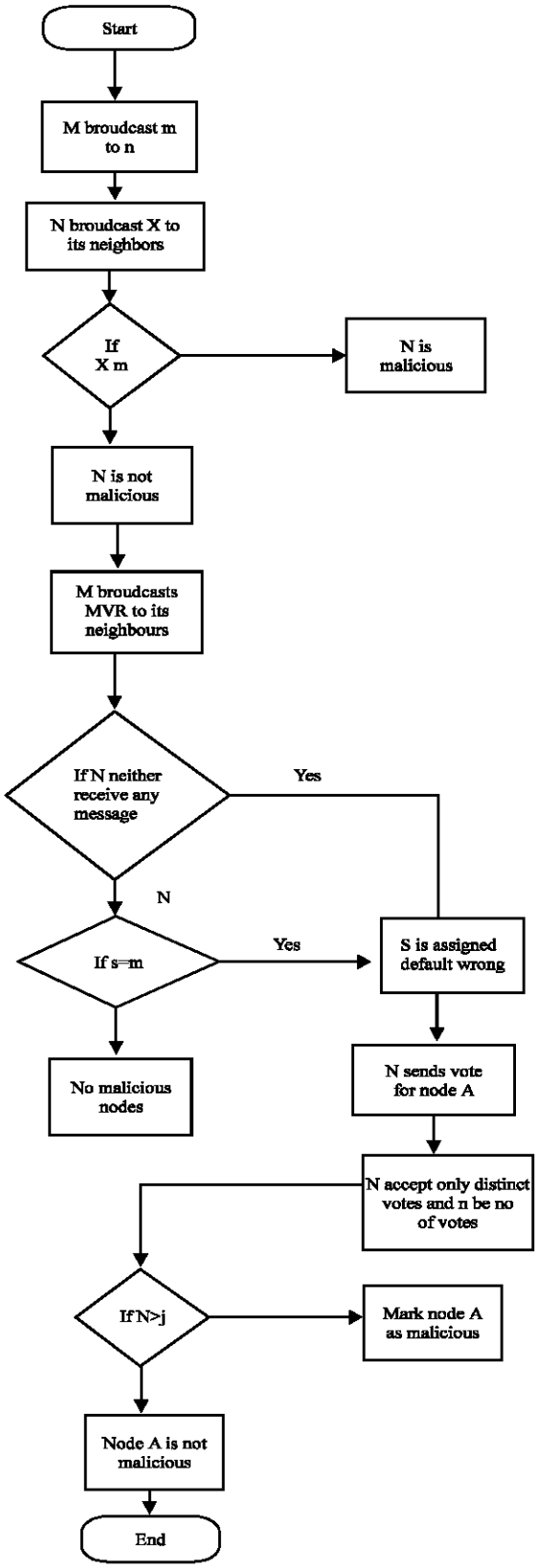

Fig. 3: Flowchart for ADCLU algorithm

Hence, our goal is to recognize out-of-band high bandwidth mode. Since, in out of band attack, monitor node don't have any connection with second malicious node. As per algorithm:

- The monitor node send original (RIGHT) message to first malicious node
- Then the first malicious node sends this message to second malicious node in other cluster
- In out of band attack, monitor node don't have any connection with second malicious node. Hence, the second malicious node does not receive any message from monitor node. Therefore, it has no intelligence to send RIGHT message to the first malicious node
- When, the monitor node sends malicious-vote request message to its neighbourhood, it receives only one vote for suspecting of the second node in other cluster from the first node
- Since, monitor node is not aware of that second node is in other cluster, it supposes that second malicious node is in the same cluster, because first node doesn't receive any messages from second node in step
- Finally, monitor node doesn't accept these nodes to be malicious nodes because n<j and uses them in routing decisions so these algorithms are failed to detect malicious nodes in this form of wormhole attack

Now, these nodes can access to network traffic and drop packets data or change the packets and send them to other nodes, etc. Hence, the threshold should consider conditions which the value of malicious-vote-request message equals to one. The algorithm has certain characteristics:

- We obtain same results for the minimum number of malicious nodes (two nodes) and more than two nodes in out-of-band wormhole attack. Hence this technique is independent of number of malicious nodes
- These malicious nodes must be isolated and repeated this IDS process several times. After gathering votes and specifying the value of j in different IDS processes, the number of wrong votes must be evaluated
- If the numbers of one vote for showing suspected node is greater than the threshold, then it is detected as wormhole attack. It means that wormhole attack is faced
- The amount of threshold depends on type of network for Consumption of energy, enough memory space for storing history of amount of j in different IDS processes, node's processing power and especially the importance of security in that network

Overall algorithm:

- Initially, a cluster is formed with a neighbourhood of nodes
- The monitor node is chosen inside the cluster using an algorithm considering the willingness and trust value of a node
- Each monitor node has nodes in the cluster as its 1-hop neighbours
- This monitor node can be used in ADCLU algorithm to detect malicious nodes in a neighbourhood of nodes where each pair of nodes may not be in radio range of each other but where there is a node among them which has all the other nodes in its one-hop vicinity
- The malicious node is detected by taking voting from all other nodes
- Once a node is marked malicious in the cluster, it is isolated from communicating with other nodes

RESULTS AND DISCUSSION

Simulation model and parameters: We use Network Simulator version 2 (NS2) to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the Trust Based Collaborative Attack Detection (TBCAD) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, mobile nodes move in a 1000 m×region for 50 sec simulation time. The numbers of attackers are varied as 1, 2, 3, 4 and 5. Our simulation settings and parameters are summarized in Table 1.

Table 1: Simulation settings

Number of nodes	60 and 100
Area size	1000×1000
Mac	802.11
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Rate	100 kb
Routing protocol	CERM
No. of attackers	5, 10, 15, 20 and 25
Antenna	Omni antenna

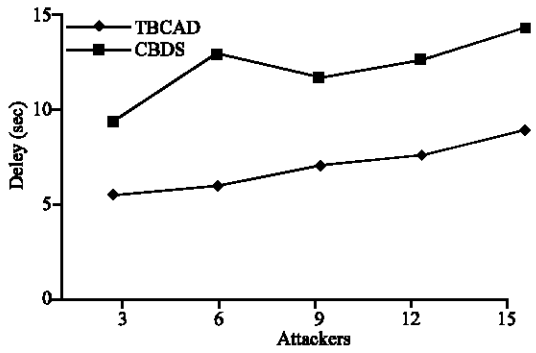

Fig. 4: Attackers vs delay

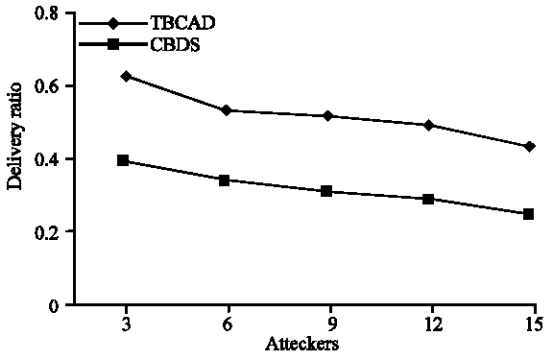

Fig. 5: Attackers vs delivery ratio

Performance metrics: We evaluate mainly the performance according to the following metrics.

Average packet delivery ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Average packet drop: It is the average number of packets dropped by the misbehaving nodes.

End-to-end delay: It is the amount of time taken by the packets to reach the destination.

Based on attackers for nodes 60: In our first experiment we vary the number of attackers as 3, 6, 9, 12 and 15. From Fig. 4, we can see that the delay of our proposed TBCAD is 42% less than the existing CBDS protocol. From Fig. 5, we can see that the delivery ratio of our proposed TBCAD is 39% higher than the existing CBDS protocol. From Fig. 6, we can see that the packet drop of our proposed TBCAD is 55% less than the existing CBDS protocol. From Fig. 7, we can see that the overhead of our proposed TBCAD is 43% less than the existing CBDS protocol.

Based on attackers for nodes 100: In our first experiment, we vary the number of attackers as 5, 10, 15, 20 and 25. From Fig. 8, we can see that the delay of our proposed TBCAD is 16% less than the existing CBDS protocol. From Fig. 9, we can see that the delivery ratio of our proposed TBCAD is 18% higher than the existing CBDS protocol. From Fig. 10, we can see that the packet drop of

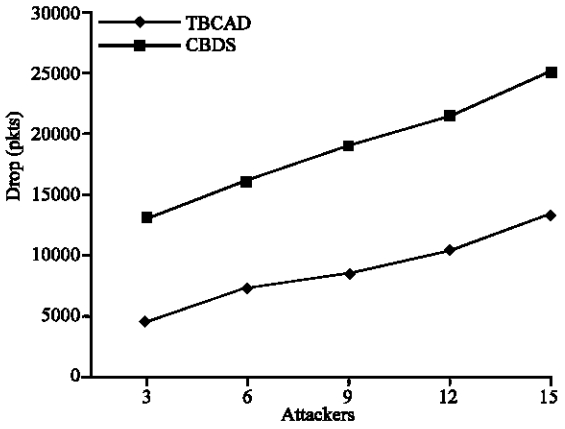

Fig. 6: Attackers vs drop

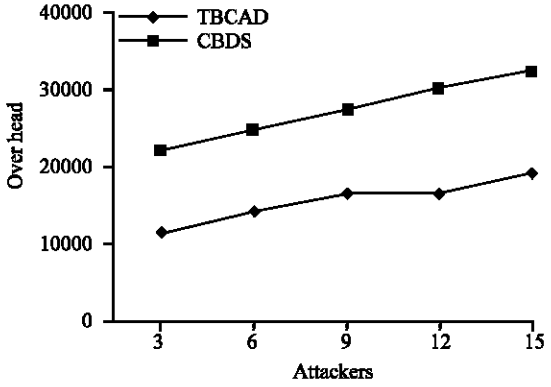

Fig. 7: Attackers vs overhead

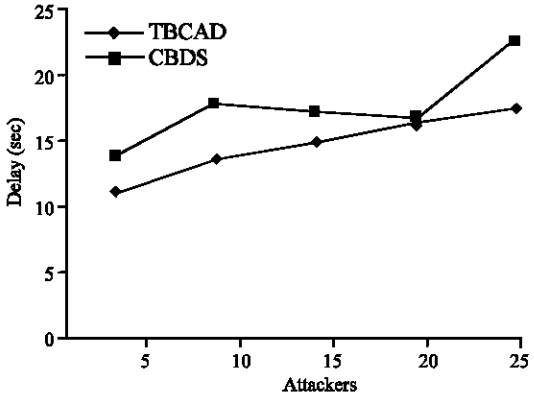

Fig. 8: Attackers vs delay

our proposed TBCAD is 36% less than the existing CBDS protocol. From Fig. 11, we can see that the overhead of our proposed TBCAD is 36.2% less than the existing CBDS protocol.

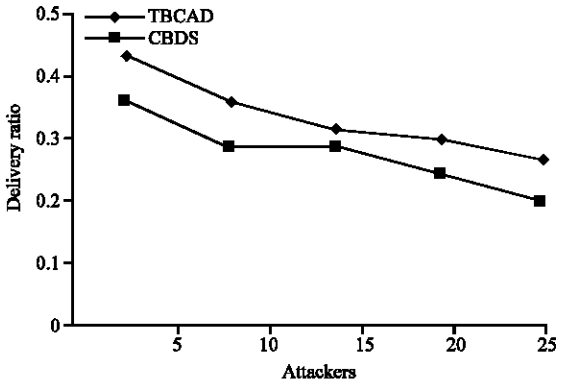

Fig. 9: Attackers vs delivery ratio

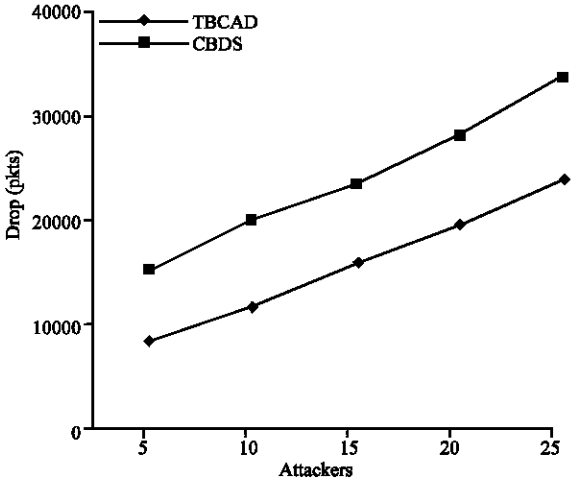

Fig. 10: Attackers vs drop

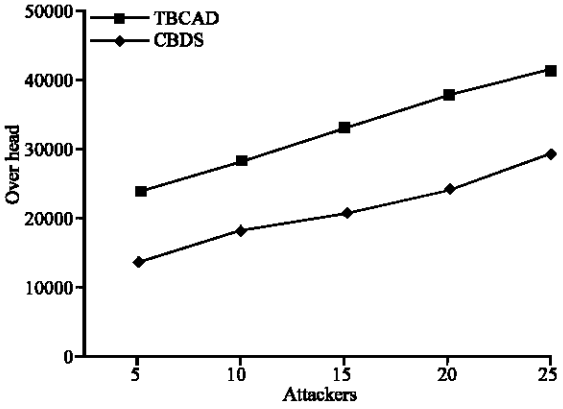

Fig. 11: Attackers vs overhead

CONCLUSION

The critical issues of MANET due to the various attacks like wormhole, black hole, grayhole and even

collaborative attacks can be detected and prevented by developing a detection scheme. Initially, clusters are formed with neighbourhood of nodes with a monitor node with all nodes at its 1-hop neighbours. This monitor node was chosen using an algorithm considering the willingness and trust value of a node. Then, we used ADCLU algorithm utilizing the monitor node to detect malicious nodes in a neighbourhood of nodes. Here, each pair of nodes may not be in radio range of each other but where there is a node among them which has all the other nodes in its one-hop vicinity. The detection was based on voting from all other nodes about a certain message. The malicious node detected is isolated and further communication with this node is stopped.

REFERENCES

Banerjee, S., 2008. Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. Proceedings of the World Congress on Engineering and Computer Science, October 22-24, 2008, San Francisco, USA., pp: 1-6.

Bhargava, B., R. de Oliveira, Y. Zhang and N.C. Idika, 2009. Addressing collaborative attacks and defense in ad hoc wireless networks. Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops, June 22-26, 2009, Montreal, QC., Canada, pp: 447-450.

Chang, J.M., P.C. Tsou, I. Woungang, H.C. Chao and C.F. Lai, 2015. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE Syst. J., 9: 65-75.

Dureja, A. and V. Dahiya, 2014. Performance evaluation of collaborative attacks in MANET. Int. J. Comput. Sci. Mobile Comput., 3: 457-465.

Gong, T. and B. Bhargava, 2013. Immunizing mobile ad hoc networks against collaborative attacks using cooperative immune model. Secur. Commun. Networks, 6: 58-68.

Mathew, R.L. and P. Petchimuthu, 2013. Detecting selfish nodes in MANETs using collaborative watchdogs. Int. J. Adv. Res. Comput. Sci. Software Eng., 3: 37-41.

Nouri, M., S.A. Aghdam and S.A. Aghdam, 2011. Collaborative techniques for detecting wormhole attack in MANETs. Proceedings of the International Conference on Research and Innovation in Information Systems, November 23-24, 2011, Kuala Lumpur, Malaysia, pp: 1-6.

Patel, M. and S. Sharma, 2013. Detection of malicious attack in MANET a behavioral approach. Proceedings of the IEEE 3rd International Advance Computing Conference, February 22-23, 2013, IEEE, Ghaziabad, India, ISBN: 978-1-4673-4527-9, pp: 388-393.

Sen, J., M.G. Chandra, P. Balamuralidhar, S.G. Harihara and H. Reddy, 2007. A distributed protocol for detection of packet dropping attack in mobile ad hoc networks. Proceedings of the IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, May 14-17, 2007, Penang, Malaysia, pp: 75-80.

Singh, U.K., K. Phuleria, S. Sharma and D.N. Goswami, 2014. An analysis of security attacks found in mobile ad-hoc network. Int. J. Scient. Eng. Res., 5: 1586-1592.

Wang, W., B. Bhargava and M. Linderman, 2009. Defending against collaborative packet drop attacks on MANETs. Proceedings of the 2nd International Workshop on Dependable Network Computing and Mobile Systems, September 27-30, 2009, Niagara Falls, New York, USA., pp: 1-6.

Yu, C.W., T.K. Wu, R.H. Cheng and S.C. Chang, 2007. A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network. In: Emerging Technologies in Knowledge Discovery and Data Mining, Washio, T., Z.H. Zhou, J.Z. Huang, X.H. Hu and J.Y. Li *et al.* (Eds.). Springer, New York, USA., pp: 538-549.