A Review Paper on Cluster Based ANT Defense Mechanism Technique for Attack in MANET

Sweety J Patel[1] Sanket Patel[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]KITRC collage, Mehsana Highway, Ahmedabad, Opposite Sindabad Hotel, Kalol, Gujarat 382721

Abstract— A selective forwarding attack is one of the most crucial security problems in MANET. Usually such attacker degrades the network performance in terms of packet loss rate, collision, and overhead. Designing MANET that can work reliably even in the presence of inside packet drop attackers is really challenging. In ant based defense mechanism we have implemented S-ACK scheme to transmit the secure acknowledgement. To detect attackers, a trust model is designed. The Forward ant agents transmit back the digitally signed SACK through the Backward Ant agent to detect any selective forwarding attack against any source node. Cluster distributes traffic among diverse multiple paths to avoid congestion, which optimizes bandwidth using and improves the sharing rate of channel. It uses clustering's hierarchical structure diverse to decrease routing control overhead and improve the networks scalability. By implementing the algorithm on the OPNET environment, the result shows that this algorithm balances the load of the network and deals with the change effectively of the network topology, and also improves the reliability, throughput and stability of the network efficiently.

Key words: MANET, Defense Mechanism Technique, S-ACK

I. INTRODUCTION

MANET nodes are resource, bandwidth and energy constrained devices. These nodes temporarily grouped to satisfy some requirements without any preplanning. When the number of nodes increased, it's very hard to manage the entire network due to its dynamic nature. In this context, nodes almost in same geographical location are grouped together to form sub group known as cluster and this simplifies the routing overhead by arranging nodes in hierarchical structure. Each Cluster consists of local manager known as Cluster Head (CH), Gateway node and Cluster members. Numerous clustering schemes are evolved by researchers and they are generally classified as secure clustering and Insecure clustering. The Insecure Clustering Schemes assumes network is in fully trusted environment, and it simply ignores the most vulnerable malicious nodes present inside and outside of the network.

In Secure Clustering schemes Trust based clustering prevent malicious node to become CH. Pure Cryptographic algorithms protect against outsider attacks but unable to find the malicious node. The Hybrid Schemes provide high level of security but it have its own overhead like consuming energy quickly. In Insecure clustering Scheme none of the clustering scheme protect against the insider and outsider attacks.

In Insecure clustering, comparing with remaining schemes, weight based clustering scheme is considered most advantageous, because in this CH is evaluated based on multiple metrics(Degree difference, connectivity, energy and mobility). Except weight based other clustering schemes considers single metric for electing CH. So in our research work proposed Secure Trust Based Clustering Algorithm(TBCA) is compared with existing Insecure Enhanced distributed weighted Clustering Algorithm(EDWCA).

A. As Dos Attack:

Here the malicious node selectively drops the packets coming from a particular node or a group of nodes causing a DOS attack for that particular node or a group of node

B. As Blackhole Attack:

Here it refuses to forward every packet thereby malicious node may forward the messages to the wrong path, creating unfaithful routing information in the network.

C. As Neglect and Greed:

the subverted node arbitrarily neglects to route some messages but still participate in lower level protocols and even acknowledge reception of data to the sender but it drops messages randomly. Such a node is neglectful. When it also gives excessive priority to its own messages it is also greedy. By delaying packets: they delay packets passing through them, creating the confused routing information between nodes. Selective forwarding is the most difficult attack to find defense mechanism.

II. RELATED WORK

A reputation based approach to handle with routing misbehavior and consist of detection and isolation of misbehaving nodes. Proposed approach can be integrated with any source routing protocol and based on sending acknowledgement packets and counting the number of data packets of active path. Also proposed approach has lesser routing overhead and better than previous similar schemes as it requires lesser number of acknowledgement packet transmission.

A mechanism for detection, mitigation of packet dropping attack based up on the co-operative participation of nodes in a MANET. The rate of packet forwarding is compared to a network with malicious nodes and without malicious nodes. Each packet is encrypted and bloom key is generated to hide the original packet. However it donot give provide methods to isolate identified packet drop nodes.

An Intrusion Detection System (IDS) algorithm against selfish node attack in MANET. Proposed IDS Algorithm identified the selfish node behavior and also blocked their misbehavior activities. The selfish node attack provides negligible network performance but when IDS was applied on attack, network performance was enhanced up to 92% and provided 0% Infection rate from attack. However there was higher normalized routing overload.

An enhanced trust mechanism for detecting such attackers and identify their victims. Then two attacker-aware protocols were designed to reroute victim nodes' packets by avoiding the attackers. A prevention routing algorithm was presented to proactively prevent the attack as a complementary defensive method for detection and avoidance approaches. Avoidance completion time was more.

A scheme of secure data transmission to forward the data safely, and detect the selective forwarding attack. The trust value of each node was determined to select a secure path for message forwarding so that the malicious nodes can be detected which are suspected to launch selective forwarding attack. The proposed scheme could find the malicious nodes. Here, an authentication framework was utilized to remove outside adversaries and ensured that only authorized nodes perform certain operations. However the weight assignment in key leads to increased overload.

A routing mechanism to combat the common selective packet dropping attack. Associations between nodes identify and isolate the malicious nodes. The Association based routing was extended to be applied over the DSR protocol to enhance the security. The scheme fortified the existing implementation by choosing the best and secured route in the network. A trust value was calculated for each node in the network to represent its reliability level. However there was reduced packet delivery ratio.

Designed a challenge and response scheme to detect the selective forwarding attack in MANETs. The scheme has two phases. One was a key distribution phase and another was a challenge and response phase. In both phases, MANET nodes were assumed to use at least two channels to transmit routing messages. Two neighbor's traffic was compared with a local one to detect an attacker. In addition the attackers could be identified using the selective attacking technique. However performance metrics were not evaluated.

A scheme to detect malicious nodes in the network responsible for triggering the Selective packet Drop attack in the network. Diffie-Hellman technique was utilized to isolate the selective packet drop attack to an extent MANET. The Diffie-Hellman algorithm provided for establishing secure channel.

A method to trace the TCP attacker after detecting the type of attack originated in the network. TCP traffic history can trace back attacker to identify the attacker and its zone. Static Cognitive Agent (SCA) and Mobile Cognitive Agents (MCA) was deployed for history collection, attack detection, attack zone identification and attacker trace back.
Various techniques have been proposed by researchers to prevent and/or detect this attack. Abbas et al. proposed a lightweight technique for detecting the forged identities of an attacker. The proposed technique works on the basis of the Received Signal Strength (RSS) to analyze whether the new node which has joined the network is legitimate or a new fake identity of a fraud node. Initially, when a new node comes inside the network, its RSS level will be low in the beginning and then it will increase gradually. On the other hand, the fraud node which is generating a new fake identity is already present in the network and not a newcomer, therefore its entrance behavior in the radio range of another node is different. Hashmi et al. presented a mechanism to detect the identity forging node which is based on device's fingerprint. Hardware-IDs of the devices carried by a mobile node can be used as a fingerprint for the purpose of unique identification of that node. The technique benefits from the fact that a node cannot forge the identities of the hardware devices that it carries. However, an authenticator node is required which can execute the authentication process on a node to verify it's hardware-ID.

A Non-centralized approach has been proposed by Tangpong et al. In their work, all nodes of the network participate in the detection procedure of the identity forging node. The detection mechanism is based on the fact that fake identities of a node travel together. In this approach, packets passing through the network are exchanged and examined by every node to find out the attacker based upon the location. However, the technique requires node positioning system so that the actual direction of the incoming packet could be found out. Also availability of directional antenna at every node is required.

III. PROBLEM IDENTIFICATION AND SOLUTION

Fig.l represents the block diagram. In this proposed ACO based defense mechanism S-ACK scheme and digitally signed scheme to transmit secure acknowledgement. A trust model is designed to detect any misbehaving node. Further, to monitor the neighboring node and information updated by ant agents, a challenge and monitoring packet which contains metrics such as random value, wake up time and verification code is transmitted by source node through the selected routing path.

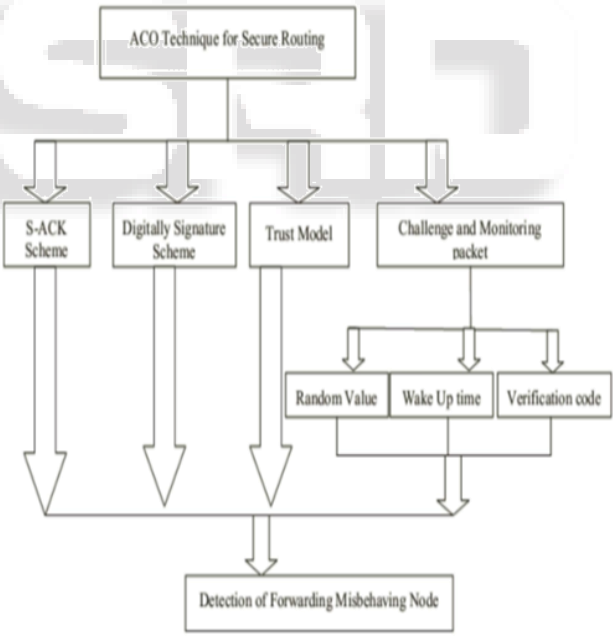

Fig. 1: Block Diagram.

A. *Ant based Defense Mechanism:*

This section describes about the enhanced secured ant based routing algorithm that efficiently detect misbehavior nodes in the network. Due to the colonial behavior of ant, ACO technique provides the optimal solution for complex operation.

B. *S-ACK:*

This section describes about the S-ACK scheme which is followed byF -Ant to deposit pheromone and detect misbehaving nodes. The main principle of this scheme is to

allow three consecutive nodes work in a group to detect misbehaving nodes. According to this scheme, for every three consecutive nodes in the route, the third node is needed to send an S-ACK acknowledgement packet to the first node to detect misbehaving nodes even in the presence of receiver collision or limited transmission power.F ig.2 represents the S ACK scheme. Here node A transmits the S-ACK data packet DSAT to the node B, then node B forwards it to node C. As node C is the third node it send back S-ACK acknowledgement packet DACK back to the node B which is forwarded back to the node A. If node A do not receive any acknowledgement packet, then node B and C are malicious node.

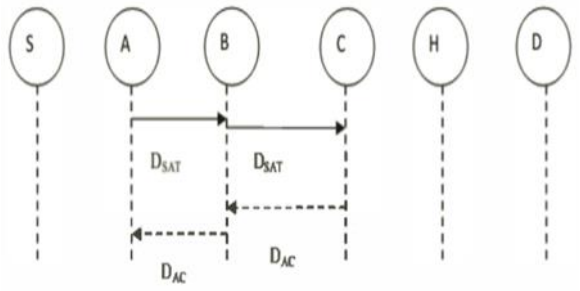

Fig. 2: Representation of S-ACK Scheme.

C. Digital Signature:

To enhance the authenticity, F-Ant transmits the digital signed acknowledged packet. As, the attackers in MANET can forge acknowledgement packets at any time, it is very important to transmit digitally signed acknowledgement and hence maintain the integrity of the data transmitted. In proposed scheme, both RSA and DSA digital signature scheme is used.

In a manner similar to other legitimate nodes, the fraud nodes also exchange the Hello packets with the other nodes. Since, each of its fake identity is behaving as an independent node, all these identities send their respective node-ID and neighbour-list pair to the cluster-head regularly. As an example, Table-I shows the node-ID and neighbour-list pairs corresponding to each of the nodes shown in Fig. 3. It can be observed from Table-I. that the following group of nodes have common neighbourhood: [{2, 3, 4, 5}, {15, 16, 17}, {10,11}].

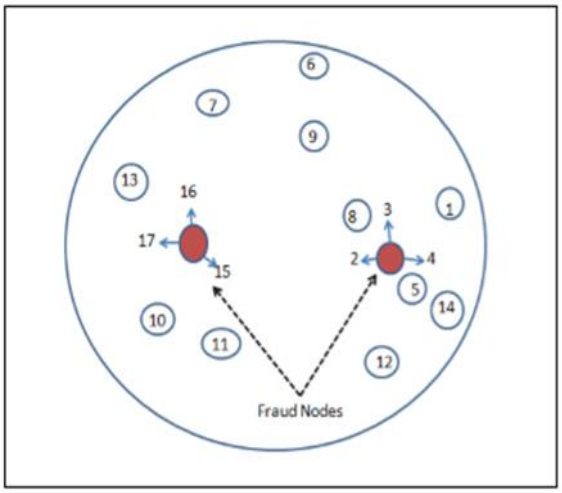

Fig. 3: Nodes Inside a Cluster at Time Instance T(i)

Neighbour List at Time T(i)	
Node-ID	*Neighbour-List*
1	{ 2, 3, 4, 5, 8, 14 }
2	{ 1, 3, 4, 5, 8, 12, 14 }
3	{ 1, 2, 4, 5, 8, 12, 14 }
4	{ 1, 2, 3, 5, 8, 12, 14 }
5	{ 1, 2, 3, 4, 8, 12, 14 }
6	{ 7, 9 }
7	{ 6, 9, 13 }
8	{ 1, 2, 3, 4, 5, 9 }
9	{ 6, 7, 8 }
10	{15, 16, 17, 11 }
11	{ 15, 16, 17, 10 }
12	{ 2, 3, 4, 5, 14 }
13	{ 7, 15, 16, 17 }
14	{ 1, 2, 3, 4, 5, 12 }
15	{ 10, 11, 13, 16, 17 }
16	{ 10, 11, 13, 15, 17 }
17	{ 10, 11, 13, 16, 15 }

Table 1: Naighbour Node List

As the time advances, the neighbour list of each node may change due to mobility. The fake identities of an attacker also travel together as a group to some other place. Their neighbourhood will also change since they might have reached to a different place. It is worth noting here that all the fake identities of a fraud node belong to a single device, because of which they will always share a similar neighbourhood among themselves i.e., their neighbour-list will be common to each other. The detection approach proposed in this paper uses the above mentioned fact that when a group travels together, the members of the groups have common surroundings or neighbours. The Detector node compares the neighbour-list of each node with the neighbour-list of other nodes to find out such a group of fake identities. The approach implemented in this work is centralised in nature because only Detector node is involved in executing the actual detection algorithm.

IV. Conclusion

In this paper we proposed an enhanced cluster based Ant Defense Mechanism for Selective Forwarding Attack in MANET. First, we have implemented S-ACK scheme to transmit the secure acknowledgement. The F-Ant transmits the S-ACK along with the digitally signed packet to reduce overhead in the network. To detect malicious nodes, a trust model is designed that defines the trustworthiness of the node based on the number of time the packet is dropped before forwarding. It can be concluded from this paper that a fraud node forging many fake identities can easily be found out using the simple algorithm proposed and implemented here. The detection method is capable of finding out more than one fraud nodes in the network. However, this algorithm generates false positives when the speed of nodes is low and simulation time is less. The approach of detection may not be suitable for the networks where the mobility of nodes is very less.

REFERENCES

[1] C. Cordeiro and P. Agrawal, "Mobile ad-hoc networking," 20th Brazilian Symposium on Computer Networks, 2002, pp. 125-186.
[2] P. Ghosekar, G. Katkar and P. Ghorpade, "Mobile ad hoc networking: Imperatives and challenges," IJCA Special Issue on MANETs, Vol. 3, 2010, pp. 153-158
[3] J.K. Douceur, "The sybil attack," Presented at the Revised Papers from the First Int.Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.
[4] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis and defences," Presented at the 3rd Int. Symp. Information Processing in Sensor Networks (IPSN), 2004, pp. 259–268.
[5] R. Agarwal and M. Motwani, "Survey of clustering algorithms for MANETs," International Journal on Computer Science and Engineering, Vol.1 (2), 2009, pp. 98-104.
[6] A. Vasudeva, and M. Sood, "Sybil attack on lowest id clustering algorithm in the mobile adhoc network," Proceedings of the International Journal of Network Security & Its Applications (IJNSA), 2006.
[7] M. Al-Shurman, S.M. Yoo, and S. Park, "Black hole attack in mobile ad hoc networks," ACM Southeast Regional Confererence, 2004.
[8] S. Abbas, M. Merabti, D. Llewellyn-Jones and K. Kifayat, "Lightweight sybil attack detection in MANETs," IEEE Systems Journal, Vol.7, 2013, pp. 236-24.
[9] S. Hashmi and J. Brooke, "Toward sybil resistant authentication in mobile ad hoc networks," In Proc. 4th Int. Conf. Emerging Security Information, 2010, pp. 17–24
[10] A. Tangpong and G. Kesidis, H. Hung-Yuan, and A. Hurson, "Robust sybil detection for manets," In Proc. 18th ICCCN, 2009, pp. 1–6.
[11] S. Hazra and S.K. Setua, "Sybil attack defending trusted aodv in ad-hoc network," Computer science and Network Technology (ICCSNT), 2012 2nd International Conference, pp.643,647, 29-31.
[12] C. Piro, C. Shields, and B. N. Levine B, "Detecting the sybil attack in mobile ad hoc," In Proc. Securecomm Workshops, 2006, pp. 1-11.
[13] S. Abbas, M. Merabti, D. Llewellyn-Jones, "A reputation based scheme to deter identity based attacks for clustered MANETs." In the 10th Annual Conference on the Convergence of Telecommunications, Networking and Broadcasting Liverpool, UK, 2009, pp. 243-248.
[14] D. Monica, J. Leitao, L. Rodrigues, and C. Ribeiro, "On the use of radio resource tests in wireless ad hoc networks," In Proc. 3rd WRAITS, 2009, pp. 21–26.
[15] C.E. Perkins, and E.M. Royer, "Ad-hoc on-demand distance vector routing," Proceeding of 2nd IEEE Workshop on mobile Computing Systems and Applications, 1999, pp. 90-100. [16] TimeComplexity (2012). "Time Complexity - Python Wiki,"[online]Available:https://wiki.python.org/moin/ TimeComplexity.
[16] Tripti Nema, "Energy Efficient Adaptive Routing Algorithm in MANET with Sleep Mode", International Journal of Advanced Computer Research.
[17] Abdelwadood Mesleh, "AODV and DSR energyaware routing algorithms: a comparative study", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 1, November 2012.
[18] K. Tamizarasu, "An AODV-based Clustering Approach for Efficient Routing in MANET", International Journal of Computer Applications (0975 – 8887).
[19] Jaya Jacob, "efficiency enhancement of routing protocol in MANET".
[20] K. Tamizarasu, "An AODV-based Clustering Approach for Efficient Routing in MANET", International Journal of Computer Applications (0975 – 8887).
[21] Mehdi Lotfi, "A New Energy Efficient Routing Algorithm Based on a New Cost Function in Wireless Ad hoc Networks", Journal of Computing, Volume 2, Issue 6, June 2010, ISSN 2151-9617.
[22] Sumathy S, "Survey of genetic based approach for multicast routing in MANET", International Journal of Engineering and Technology.

