Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1657 - 1666
Received 15 April 2021; Accepted 05 May 2021.

Strong Security Scheme for Single Node and Colluding Nodes Byzantine Attacks in MANETS

R.Sivakami [1], S. Chiranjith Raghava [2], Venkatesh R [3]

[1]Associate Professor, Department of Computer science and Engineering, Sona College of Technology, Salem, Tamilnadu. Email Id: shivasona07@gmail.com

[2]UG Scholar, Department of Computer science and Engineering, Sona College of Technology,
Salem, Tamilnadu. Email Id: raghavchiranjeet@gmail.com

[3] Professor, Department of Information technology, PSNA College of Engineering and Technology, Dindigul, Tamilnadu.Email Id: rlvenkatesh@gmail.com

Abstract

Mobile Ad Hoc networks are the wireless networks and are established spontaneously without any fixed infrastructure to connect the devices for communication and sharing resources. Almost all of these devices are connected using radio network and this radio network is vulnerable to attackers of all kinds from novice to specialists and all sorts of attacks from active to inactive attacks. Though MANETs have profound use in many fields, the major application areas are disaster recovery, military field, IoT, VANETs and also used in crucial and life saving areas of health care systems. One of the active attacks is Byzantine attack and it has various forms such as black hole, worm hole and distributed denial of service. These attacks can be executed by single node or by multiple colluded nodes to stamp the entire network. The system presented in this paper provides a mechanism for reliable and secured communication against all forms of Byzantine attack with strong authentication. The nodes actions are monitored in each and every layer and the feedback of the nodes is generated as weights in Kirchhoff's matrix. This is passed to the contact layers used in network activities from route establishment to message transmission. This cross layer feedback along with other secured mechanisms defends against all forms of Byzantine attacks in all stages from detection and recovery to prevention.

Keywords: Byzantine attacks, Black hole, wormhole, network overlay, security, Authentication, MANETS, IoT

1. DATA COMMUNICATION IN MANETs

1.1 Byzantine Attacks

MANETS are vulnerable to attackers and Byzantine attacks are the most harmful and hazardous one among the active attacks. Byzantine attacks are the major potential threats that shatter the proper functioning of the system. Byzantine attacks are active insider multilayer attacks and they are carried out by the authenticated nodes that are very much aware of system functions. The malicious nodes can execute attacks as single handed or by colluding with other attackers. Byzantine nodes exhibits many types of network attacks such as giving incorrect routing information, forwarding packets in the wrong non optimal route, dropping

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1657 - 1666
Received 15 April 2021; Accepted 05 May 2021.

packets, giving false information to neighbors, creating routing loops and collude with other adversaries, create a worm hole with an illusion of minimal path length and later dropping all packets routed to this tunnel. These Byzantine attackers are hard to find as they randomize the behavior quite often. They carry over their attacks in all layers of the network. In network layer, these attackers destruct the data transmission phase and in MAC layer it affects distributed coordination function DCF and jams the RTS, CTS and ACK signals. These nodes also reduce its normal back off time and access the channel frequently to prevent the bandwidth usage of benign nodes. Attacks on MAC layer due to selfish behavior of nodes is given by Kyasanur et al. [4]

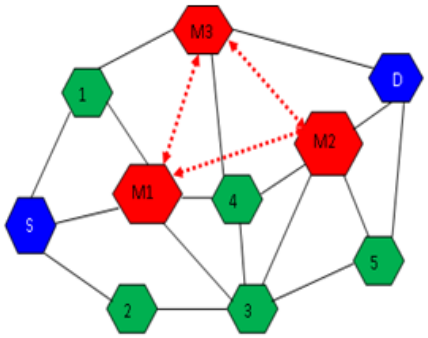

Figure 1. Byzantine Colluding Node Attacks

The detailed study Byzantine attacks and how it affects the network is given in [11, 12]. Figure 1 depicts the colluding node attacks where two or more malicious nodes jointly execute the attacks. Black hole is the single node attack that drops all received information, worm hole is the attack jointly executed by two nodes; distributed denial of service is the one when more than two nodes are in attack. The intensity of damage caused by these attacks is high and necessary detection and preventive measures should be carried out to retain the reliability of system. Lot of research is done in this area of security but all of them deal with securing at any one part or specific layer especially the routing and communication protocols of networks. Papadimitratos et al. [7, 8] did a fruitful work for securing MANETs from Byzantine attacks at the network layer. No work has been carried out so far to secure the system from Byzantine attackers at the other layers of MANETs.

Security is not a single point of protection to the system against faults and threats. Any security scheme has to consider all possible points susceptible to attacks while addressing multilayer attacks. The principle security scheme should consider attacks at networking layer and communication phase. There are no dedicated components like routers or central coordinators such as base stations and access points to overcome the hurdles created by misbehaving nodes of MANETs. Nodes have to take care of these routing and message forwarding activities. Resource sharing nodes have to rely upon other nodes of network if they are not within the direct transmission range of each other. All nodes are not reliable and some may exhibit stealthy behavior intentionally due to selfishness. Byzantine attacks are multilayer attacks and as a protective measure data communication is secured first.

A secured routing and authentication is proposed and a complete system with all three parts such as detection, prevention and recovery from all forms of Byzantine attacks is explained. The protection method which blocks the attackers and a fast recovery method to retain the normal operability of network are explained. Paper concludes with performance evaluation of secured communication with fast failure recovery.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1657 - 1666
Received 15 April 2021; Accepted 05 May 2021.

1.2 Procedure for Secure Data Communication with strong authentication

Figure 2 represents the overall architecture of the system. Threshold limits are set initially based on the security requirement of the application. Get the security requirement of the MANET Application. (0-Normal protection, 1-High level Protection).Set the threshold based on the environment and the viability of security threats. (Threshold between 0 and 1).

i) Source node initiates data transmission with the feedback sent by MAC layer. MAC layer creates the feedback of nodes as a weight vector and information about current topology as a Kirchhoff matrix and pass it to higher layers. The details of Kirchhoff matrix and its use in MANET are given in [3] and [13].

ii) Source node analyzes the feedback and computes predicted node length and number of edge disjoint paths from source to destination. RREQ with [query Id, (source, destination, timestamp, TL, pl, pn), $K_{S,T}$] is fed as input to the hash function. MAC is encrypted with K_T^+.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1657 - 1666
Received 15 April 2021; Accepted 05 May 2021.

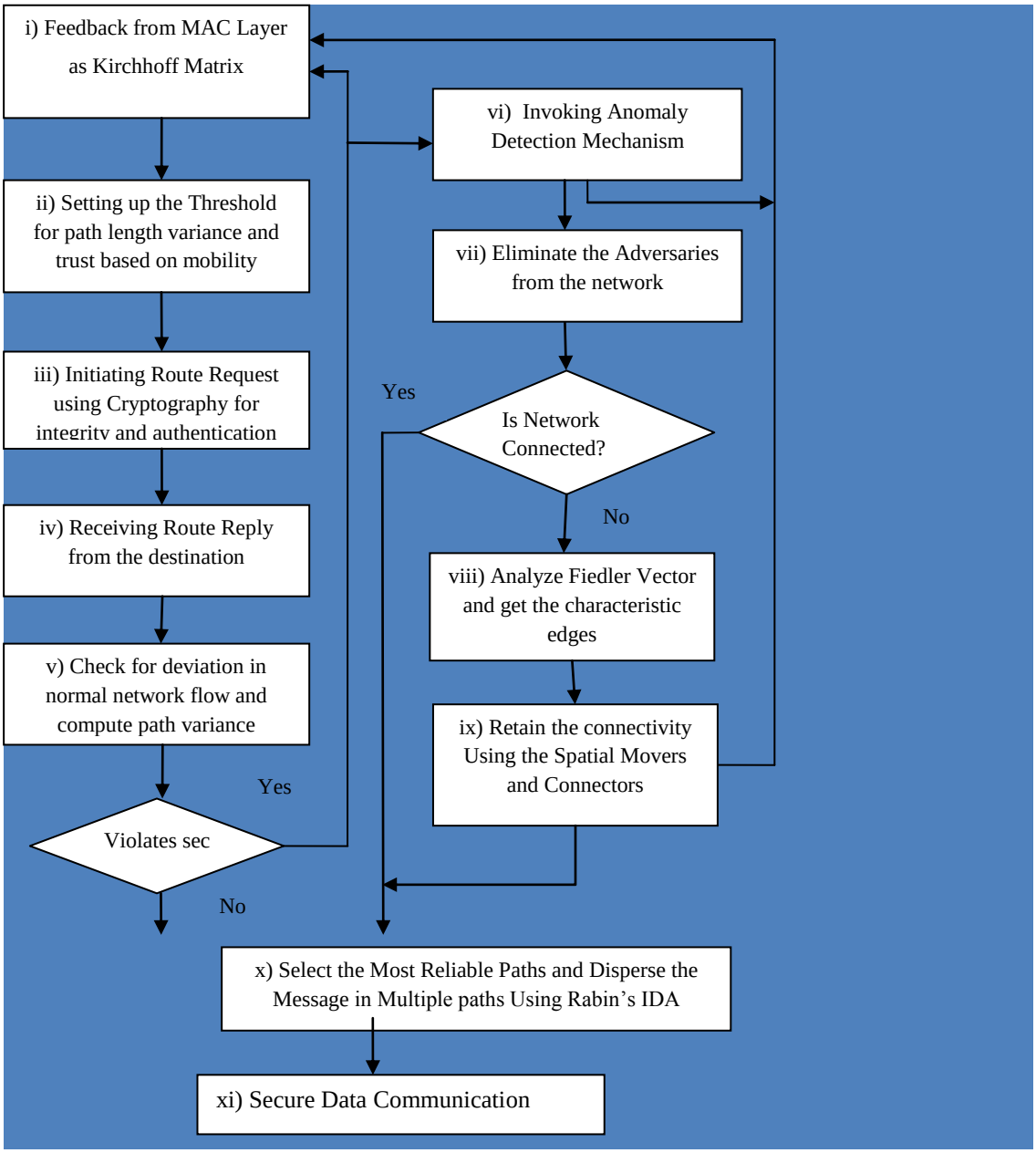

Figure 2. Overall Architecture of Secure Communication

iii) Intermediate nodes add their id and forward route request towards destination. Malicious nodes cannot tamper the route messages because only destination can decode the message.

iv) Source node waits for tolerable delay time for the arrival of route reply. Route reply is also secured in the same way as route request.

v) When delay time exceeds the limit, may be due to Byzantine black hole attack, source node starts querying the nodes lay on suspected path to find out the faults.

vi) Applying anomaly detection mechanism to find out the benign and faulty nodes.

vii) All nodes have a history of received and forwarded route requests, route replies and a state table to reflect the behavior of the nodes as kept in MAC layer. Each node maintains a route forwarding table till the source completes its transmission. After receiving ACKS the entry in the forwarding table is discarded and updates are made

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1657 - 1666
Received 15 April 2021; Accepted 05 May 2021.

into the status of loyal and benign nodes. The adversaries are discarded from the routing path and from further activities of the network.

viii) The cross layer feedback predicts cut vertices and stability of network. The nodes and their connectivity and positions are analyzed.

ix) If the attackers are the cut vertices then network will be disconnected soon. Spatial movers and connectors are called to move to the particular distance for retaining connectivity.

x) The message is encrypted and added with minimal redundancy to tolerate the data loss due to movement of nodes and the adversarial actions of malicious nodes. The redundant message is dispersed in multiple paths using Rabin's dispersal algorithm.

xi) Data can be reconstructed even if there is a loss of data within the allowable limit. For dispersing the message in more reliable paths, an adaptive information dispersal algorithm using Kirchhoff matrix is used.

2. AUTHENTICATION OF NODES AT MAC LAYER

There are three ways to authenticate nodes at MAC layer. The nodes can be authenticated using shared secret key and public key infrastructure or can use certificate authority. Public and private key generation by the nodes and authentication of keys through certificates is described by Capkun et al. [2]. Public key cryptography given by Rivest et al. [10] is widely used for network and information security. The public key cryptography uses pair of keys – private key known only to the user and a public key known to others. If the nodes that are going to be a part of MANETs are well known before establishing the network like in military MANETs then the pre allocated code identifies them uniquely in network. MAC layer uses this code for authentication purpose. When nodes join the network, they have to broadcast their ID.

2.1 High Level Authentication Scheme for Security Sensitive Applications

Wireless communication and ad hoc establishment of MANET has more security breaches than standard firewall based networks with fixed infrastructure and strong intrusion detection system. MANETS applications play a major role in military operations where unmanned army vehicles are used for surveillance and in battlefields. Intruders come up with new ways to break the security walls and gather invaluable information. It is essential to prevent the intruders and admit only authorized systems in the network. The security needed for military MANETs differ from normal networks. The key maintenance for authentication phase is stronger for military MANETs. Groups are maintained to represent the hierarchy of army system.

2.2 Authentication by Group Leader

Steps carried out in authenticating the node A by group leader L in a group are given in the following four equations.

$$\boldsymbol{Node\ (A)} \xrightarrow[\boldsymbol{K_L+(A,R1)}]{} \boldsymbol{Group\ Authenticator(L)} \quad (1)$$

$$\boldsymbol{Node\ (A)} \xleftarrow[\boldsymbol{K_{A+}\ (K_{A,L},A,(R1*pA),R2)}]{} \boldsymbol{Group\ Authenticator(L)} \quad (2)$$

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1657 - 1666
Received 15 April 2021; Accepted 05 May 2021.

$$Node(A) \xrightarrow[K_{A,L}(A,(R1*pA+1),(R2*pA)}]{} Group\ Authenticator(L) \quad (3)$$

$$Node(A) \xleftarrow[K_{A,L}(A,K_{A+}(K_{A,GC}))]{} Group\ Authenticator(L) \quad (4)$$

Nodes are assigned with individual ID in a group. As given in equation (1), the node intimate its ID -**A** and a random number-**R**1 generated as challenge to the authenticator encrypted by authenticator's public key- $\mathbf{K}_{L}^{+}$. The message can be decrypted only with authenticator's private key which is known only to leader. So anomalies cannot reply the challenge.

As a response to the challenge, the leader decrypts the message and a product of the part of the node id- **pA** and the random number-**R1** generated by the node is computed. The response along with a random number-**R2** and the secret key-$\mathbf{K}_{A,L}$ is sent back as a reply to the node as challenge. The whole information is encrypted by the node A's public key- $\mathbf{K}_{A}^{+}$ as represented in equation (2).

The node replies in the same manner as given above and encrypt it now by using the secret key shared with the leader- $\mathbf{K}_{A,L}$. The node's reply is as in equation (3). Finally after these two sides of verification, the group authenticator issues a group code-$\mathbf{K}_{A,GC}$ to member nodes as illustrated in equation (4). Whole authentication process is a strong authentication process and able to resist all kinds of attacks in getting the group code. The Diffie Hellman secret key sharing is used.

3. SETTING UP THRESHOLD FOR PATH LENGTH VARIANCE AND TRUST FACTOR

Only authenticated nodes are present in the network during this phase and external intruders are filtered to the maximum at the link layer itself. But the authenticated insiders may carry out Byzantine attacks. So the nodes are to be monitored and controlled in route establishment and data forwarding phases too. The allowable limit of deviation from normal networking behavior is set as threshold.

The source node has information about the topology from MAC layer and aware of malicious nodes behavior. Before sending route request, the source estimates path length between end nodes. However estimated path length is not accurate due to mobility of nodes. So an acceptable threshold for deviation in path length and trust factor of nodes is set considering the susceptible environment where the nodes are mounted. Few of the sample factors are mobile nodes may be vehicles or devices carried by human, geographical location, and purpose of launching MANETs. The author Ryma Abassi (2018)[15] has proposed a way to compute the trustworthiness of the nodes from their past actions. Here we have used an analytics of the nodes behavior and set a threshold to compute its genuineness.

If nodes execute wormhole attack then the path length returned will be smaller than the actual length. The malicious nodes respond correctly to the routing phase and perform attacks only in data transferring phase can easily be caught by difference in trip time variation. Threshold set for path length variation is as depicted in equation (5).

$$\Delta_l = \left| \frac{\text{Predicted Path Length - Actual Path Length}}{\text{Predicted Path Length + Actual Path Length}} \right| \quad (5)$$

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1657 - 1666
Received 15 April 2021; Accepted 05 May 2021.

The Δ_l in equation (5) always lies between 0 and 1. Maximum value for Δ_l is tuned as threshold for high mobility network and moderate for low mobility networks. For example if the predicted path length is 20 and due to high mobility and the actual path is half of it that is 10 , then by applying the formula given in equation (6), Δ_l computed is 0.3. So the value 0.3 can be the maximum threshold for high mobility and .2 for low mobility network.

$$\Delta_l = \left|\frac{20 - 10}{20 + 10}\right| = 0.3 \quad (6)$$

Distinct threshold for trust factor is set for anomaly detection. Here the trust threshold is a function of route errors, packet lost, delay variation and the packet frequency as depicted in equation (7). Like in setting threshold for path length variation, network condition is considered and various values are set for different situations. It allows normal loss and delay due to congestion, error prone wireless medium without fixed infrastructure. Source node transmits the data packets when threshold is below the maximum value.

$$\Delta_T = f(r_e, l_p, \Delta t, \Delta p) \quad (7)$$

4. SECURE ROUTE ESTABLISHMENT

Establishing secured routes, route request processing by intermediate nodes and overcoming the routing attacks using cryptography are explained in this section.

4.1 Route Request Generated by Source Node

Source node generates route request to defend various attacks carried out by adversaries in routing.

$$H = MACK_{S,T}(S, T, Q_{id}, Timestamp, TL) \quad (8)$$

$$< RREQ, S, T, Q_{id}, Timestamp, TL, nl, K_{T^+}(pl, pn, H) > \quad (9)$$

The fields are added for the following reasons. S, T identifies the source and destination respectively and Q_{id} is generated for differentiating route request from the same source to destination. The timestamp along with S, T, Q_{id} identifies the request uniquely in the whole routing process. Route request contains the information as given in equation (9). Field TTL represents time to live to avoid routing loops. The predicted number of edge disjoint paths and length of the shortest path along with hash value is encrypted by destination's public key.

The message digest computed using the secret key shared between S, T and query parameters as in equation (8) is fed as input and passed to the destination for verification. This MAC computed and the secret information shared with destination is encrypted by the destinations public key so that only destination can view the details. Route request is secured from route modification, fabrication, and cache poisoning attacks through the encryption and message digestion security methods of cryptography. The authentication and non repudiation is assured by the secret key usage of route request and it prevents the attacks from generating false request.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1657 - 1666
Received 15 April 2021; Accepted 05 May 2021.

The hashing function prevents unauthorized modification and authorized control is guaranteed by public key encryption of destination. Time Interval field of route request avoids the routing loop attacks. Source adds it's id in the node list – **nl** and broadcast the request.

4.2 Route Request Handling by Intermediate Nodes

Intermediate nodes receive the route request and check whether the query has been processed by them already. The nodes maintain a routing table for a period of time and refresh the table periodically. If there is no matching entry for **S, T, Q_{id} , timestamp and TL** combination then a new entry is made and the node add itself in the node list of route request and broadcast the request. The route request is discarded if it already exists in the routing table.

4.3 Route Reply by Destination

The destination on receiving the route request checks for integrity and then saves the route and propagate it to source after hashing the node list-**nl** along with actual number of paths-**an** and path list-**al** received for the request. The hash function- **H** and route reply-**RREP** are given in equations (10) and (11).

$$\mathbf{H} = \mathbf{MACK}_{\mathbf{S,T}}\,(\mathbf{S}, \mathbf{T}, \mathbf{Q_{id}}\ , \mathbf{Timestamp}, \mathbf{nl}, \mathbf{al}, \mathbf{an}) \qquad (10)$$

$$< \mathbf{RREP}, \mathbf{S}, \mathbf{T}, \mathbf{Q_{id}}\ , \mathbf{Timestamp}, \mathbf{TL}, \mathbf{nl}, \mathbf{K}_{\mathbf{S}^+}\,(\mathbf{al}, \mathbf{an}\ , \mathbf{mr}, \mathbf{H}) > \qquad (11)$$

If there are any malicious activities found then they are recorded and passed as a misbehaving report - **mr** to the source for further processing in anomaly detection and recovery processes.

5 DETECTION AND RECOVERY FROM BYZANTINE ATTACKS

5.1 Detection of Byzantine Attacks

Encryption, authentication and message integrity cryptographic methods are enough for outside attackers to ensure security. The Byzantine attackers are inside attackers and all are authenticated nodes. So the authentication and data integration mechanisms are not enough to identify the attackers. A collaborative mechanism to detect and isolate the misbehaving nodes or faulty nodes in mobile ad hoc network is proposed. Since there is no centralized control system, the protocols that work with the cooperation of all the nodes as a sort of distributed protocols improves the quality of service than that of any centralized protocols. To strengthen the security, a centralized control is given to the source node which initiates the communication and it becomes a commander of rest of nodes till the end of transmission.

The detection mechanism is based on enquiry sent to the nodes and analyzing replies with the information already had. Timeouts are set for receiving valid acknowledgements. The delay in receipt may be due to either malicious or non-malicious causes. When the trust threshold calculated as in equation (5) or the route path threshold as given in equation (7) crosses the set limit, system starts sending probing signals to the nodes in the suspicious path. Source has the authority to enquire network nodes. It asks for the suspicious nodes to send the received list, forwarding list and neighboring list of the nodes. Malicious nodes may give false reply.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1657 - 1666
Received 15 April 2021; Accepted 05 May 2021.

The source node will have topological information of the network by this time. The nodes performing single node byzantine attacks can be easily traced out from the search analysis. The detail given by the malicious nodes will differ from its neighbors.

Detecting Byzantine worm holes is also made easy. When the nodes involved in worm hole, they advertise shorter path normally one hop distance between them which does not exists actually. The path length given by the attackers is less than the actual path since the adversaries have established a tunnel using virtual link between them and omitted the benign nodes. The worm hole is also present in the path between source and destination. The length of shortest path is known to the source that has been computed from the cross layer feedback. Destination registers a worm hole attack on the receipt of path less than the shortest one.

The adversaries are enquired for routing and forwarding information and compared with that of its neighbors. The malicious nodes identified are omitted in the further networking activities and are removed from the network. The report on such nodes is informed to other nodes of network to protect the MANET from adversaries. Wormhole detection mechanism with various components like GPS, hop count, time, route reply and route request is given by Muhammad Imran et al**.[6]**.They also discussed the pros and cons of applying these components in wormhole detection.

5.2 Recovery

The wireless medium is more susceptible to numerous attacks than wired medium and there is always a need for secure routing protocols. Instead of transmitting message in single path, splitting the message with added redundancy and sending the message in multiple paths provide security and reliability for the communication. Data replication is the basic mechanism to recover from the loss and how it is applicable in MANET to recover data from loss due to malicious activities is explained by Takahiro Hara [14]. Multiple paths between source and destination are selected from the available topological information. For reliable and secured paths, the topological information is retrieved from Fielder vector and is explained in [13]. The topology updating algorithm should be aware of nodes mobility. The multipath message transmission also aids to minimize congestion of the network and it has been proved by Banner & Orda [1].The efficient data dispersal and network code for dispersion are given in [5,9].

CONCLUSION

The proposed work identifies and blocks Byzantine attacks, a kind of crucial insiders attack. This detection mechanism yields high performance by identifying the characteristics nodes and edges from the Kirchhoff's matrix and steps taken to avoid the malicious nodes in the path. This work has been done in [13] and presents a solution to suppress and block all forms of Byzantine attacks including wormhole attacks. Very strong authentication to detect the malicious nodes is presented in this paper.

Loyal nodes are identified by a collated code and is intimated during communication channel establishment phase of MAC layer and this authenticate the nodes as single sign on for entering into the security ring. Nodes which provide this code can take part in further communication and only their entries are noted as loyal nodes in the ARP table, and the intruders are eliminated. Intruders or external attackers are not aware of the code, so they are

noticed and rejected out in channel allocation phase and further processes presented provides a secured platform for all kinds of applications build over MANETs and use MANETs such as e-commerce using IoT, military applications, government services and industrial sectors . Nektaria and Jingyue [16] have brought the cyber attacks executed by AI and they are hard to predict and control. This work will be enhanced to address the AI based attacks and smart detection and prevention methods to provide reliability in this AI based Cyber Era.

REFERENCES

1. Banner R & Orda A 2007, "Multipath Routing Algorithms for Congestion Minimization", IEEE/ ACM Transactions on Networking (TON), vol.15, issue.2, pp.413-424.
2. Capkun S, Buttyan L & Hubaux J- P 2002, " Self-Organized Public Key Management of Ad Hoc Networks", Proceedings of ACM International Workshops on Wireless Security.
3. Joseph Fehribach D 2014, "Matrices and their Kirchhoff Graphs", ARS Mathematica Contemporanea, WPI Mathematical Sciences, vol.9, pp.125-144.
4. Kyansanur P & Vaidya NH 2005, "Selfish MAC Layer misbehavior in Wireless Networks", IEEE Transactions on Mobile Computing, vol.4, no.5, pp.502-516.
5. Lin SJ & Chung WH 2012, "An Efficient Information Dispersal Algorithm for High Code Rate System over Fermat Fields", IEEE Communications Letters, vol.16, n0.12, pp.2036-2039.
6. Muhammad Imran, Farrukh Asslam Khan, Tauseef Jaml & Muhammad Hanif Durad 2015, " Analysis and Detection Features of Wormhole Attacks in Manets", Elseveir, Procedia Computer Science. Vol.56, pp.384-390.
7. Papadimitratos P & Hass Z J 2002, "Secure Routing for Mobile Ad Hoc Networks", Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, pp.193-204.
8. Papadamitratos P , Hass Z J & Sirer E G 2002, " Path set selection in mobile ad hoc networks ", ACM MobiHoc, pp.1-11
9. Reed I S & Solomon G 1960, "Polynomial Codes over finite field", Siam Journal on Applied Mathematics, vol.8, no.2, pp.300-304.
10. Rivest R L, Shamir A & Adleman L 1978, "A method for obtaining digital signatures and public key cryptosystems", Commun ACM, vol.21, no.2, pp.120-126.
11. Sivakami R, Kadhar Nawaz G M 2015, " Adaptive IDA to protect message transmission against Byzantine attacks", International Journal of Applied Engineering Research, vol.10, no.5, pp.4084-4088.
12. Sivakami R, Kadhar Nawaz G M , " Secured Communication of MANETs in Military", 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET), IEEE Xplore, pp.146-151.
13. Sivakami R, Kadhar Nawaz G M , " A Radical Block to Byzantine Attacks in Mobile Ad Hoc Networks", 2016 Wireless Personal Communication, vol.87, no.2, pp-485-497.
14. Takahiro Hara & Sanjay Madira K ,"Data Replication for improving accessibility in Ad Hoc Networks", IEEE Transactions on Mobile Computing, vol.5, no.11, pp.1 515-1532
15. Ryma Abassi (2018) Dealing with Collusion Attack in a Trust Based MANET, Cybernetics and Systems, 49:7-8, 475-496, DOI: 10.1080 / 01969722.2018.1541598
16. Nektaria Kaloudi , Jingyue Li, " The AI –Based Cyber Threat Landscape: A Survey", ACM Comput.Surv., Vol.53,No.1, Article 20, Feb 2020.