# Byzantine Attacks and its Security Measures in Mobile Adhoc Networks

Geetha.A, and Sreenath.N

*Abstract*—**Mobile Adhoc networks(MANETs) are gaining popularity due its rapid deployment nature and ease to establish without any pre requirements. These are widely used in enormous number of applications especially in military and disaster recovery areas where secured communication is most important. Due to the medium used by it, resource limitation and dynamic topology ,it is more prone to variety of security attacks. Among them the attack by the insider compromised nodes namely byzantine attacks are very hard to predict and more dangerous. It reduces the overall network performance by affecting the trusted routing in various manners. The byzantine nodes drops the packets selectively ,pretend to be an intended intermediate node and so on and thereby challenges the reliability of the network and the participating nodes. This paper tries to discuss the major types of routing protocols ,types of security attacks, byzantine attacks and its types, and analyse the foremost categories of solutions suggested by the researchers to mitigate the byzantine attacks in the field.**

*Keywords*— **Byzantine attacks, MANETs, reliability, security.**

## I. Introduction

In current scenario wide usage of mobile devices and availability of wireless network services made communication faster and cheaper. These wide ranges of technologies made the current business strategy simpler, though they have also introduced lot of security vulnerabilities. Mobile Adhoc Network (MANET)is a kind of wireless network which is formed arbitrarily by a set of mobile nodes which are within the range of each other without any central administrator. As the network is formed on the fly and there is no authority to monitor and control the activities carried out by the participating nodes, it is more vulnerable to security threats compared to wired networks and wireless networks with access points.

Manets are widely used in situations where there is a not possible to have infrastructure network like in tsunami affected areas or setting a network is costlier to serve the required temporary purpose. Minimal configuration, rapid deployment and no need of a central governing authority make ad hoc networks suitable for emergency situations like natural disasters, military conflicts and emergency medical situation. The group of available mobile nodes which are within the range of each other forms a network communicate with each other and uses multihop routing strategy to communicate with the other nodes which are not within their range. Node Mobility which leads to dynamic topology, bandwidth constraints(limited bandwidth),error prone shared channel ,and resource constraints such as battery power of nodes are the major design issues of secured routing protocols in Manets.

In Manets secured routing becomes a real challenge since the nodes which are not familiar in past may establish a network without any central administrator. The well known early adhoc network routing protocols like AODV,DSDV establish communication paths by assuming that all participating nodes are trustworthy and thus routing is highly reliable , which is not always true due to various reasons. Wireless links are highly vulnerable to active impersonating and passive snooping. The network is more prone to insider attacks as well outside attackers. By the realization of the issues related to routing process and the need for providing security in routing, research community have started developing secured routing protocols in recent past.

This paper is structured as follows. Section 2 discusses the types of routing Protocols, section 3 discusses the major types of security Attacks in Manets, section 4 discusses about byzantine attacks and its various forms, section 5 elaborates the major categories of existing byzantine mitigation mechanisms ,section 6 discusses the major performance metrics taken by researchers to analyse the performance losses of ad hoc networks and finally section 7 concludes the study.

## II. Types Of Routing Protocols

Routing protocols of Adhoc networks can be broadly classified in to three major types 1. Proactive, 2.Reactive, and 3.Hybrid protocols.

*Proactive protocols*: Also known as Table driven protocols. In this type of protocols, nodes exchange the topology information periodically amongst them and maintain a routing table to decide the path to forward the packets between sender and receiver and to exchange data amongst them. Optimized Link State Routing protocol(OLSR),DSDV are some of the popular protocols of this kind. The major advantage of these kind of protocols is less time consumption to establish paths and the drawback is large bandwidth consumption and power consumption to store the table information and to exchange the control packets.

***Reactive protocols:*** Also known as on demand protocols. The routes will be established based on the need by exchanging control packets between the nodes. Adhoc On Demand

Manuscript received December 20, 2015.

F. A. Author is the researcher in the Computer Science and Engineering Department, Pondicherry Engineering College, Puducherry,India.

S. B. Author is a Professor in the Computer Science and Engineering Department, Pondicherry Engineering College, Puducherry,India.

http://dx.doi.org/10.15242/IJCCIE.AE0116013

Vector(AODV) ,Dynamic Source Routing (DSR) are few of the popular protocols of this category which is widely used by the research community. The major advantage is less communication overhead as routes are established on demand and the major drawback is high latency in route establishment.

***Hybrid protocols***: Also called as hierarchical routing protocol, it is a combination of both proactive and reactive routing protocols. Route establishment is done by involving proactive mechanism and reactive schemes are used in further data exchange process stages. Zone Routing protocol (ZRP), Fisheye State Routing (FSR)are the popular protocols of this category. The major issue with this kind of protocols is that the performance is unpredictable; packet delivery ratio varies depending on the number of nodes in the network and their mobility speed.

All the three above stated kinds of routing protocols can be either unicasting or multicasting in nature and are id based. The routing algorithms were developed by assuming all the participating nodes are trusted and are reliable which is not feasible due to the nature of the Manets.It makes the adhoc networks to be as unreliable networks to use mainly in critical situations like military. Thus by realizing the need of security ,lot of routing protocols based on the standard set of earlier protocols as well a new set of protocols of its own kind have been proposed[2].

## III. Major Types Of Attacks In Manets

Security attacks can be broadly classified in to two types: active and passive. The main aim of the active attacks is to destroy or modify the original data transmitted or tries to persuade the regular functioning of the network. Passive attacks do not persuade the normal network function; it aims to interfere the network and tries to read the data that is transmitted over the network without modifying any data. It challenges the confidentiality of the network if the actual data is interpreted. It is very difficult to detect the passive attacks as it won't affect the normal functioning of the network.

The attackers can be categorized into: Insiders and outsiders. If the malicious nodes from outside of the network attacks the network nodes by snooping the IDs and pretend to be an authorized node, the privacy and authenticity of the network can be compromised and are called as outsider attacks. Once the IDs are discovered, activities like modification of the original messages, flooding of erroneous routing information, replaying the old routing messages with the intention of causing extreme traffic load in the network will be carried out in order to deplete the resources. The active or passive attacks that are performed by the compromised internal nodes by tracking its neighbors, flooding the wrong false message on routing and so on is called are as insider attacks. These are more hazardous than outsider attack and are too difficult to trace and mitigate such attacks as they are the active members of the network. These attacks are also known as byzantine attacks.

External attacks that perform injection or modification of data packets and control packets, does eavesdropping are easy to avoid by using conventional cryptography encryption, integrity and authentication mechanisms. Whereas compromised inside adversaries are not possible to be discriminated and eliminated in network functionality by using simply authentication mechanism alone [1].

***Security Attributes:***

Authentication, access control, availability, confidentiality, integrity, and non-repudiation are the set of security attributes that ensures the security which can be obtained by following a group of procedures, processes and systems. In order to obtain the listed attributes Key Management, trust based solutions and mathematical models are proposed by the research community.

## IV. Byzantine Attacks

Attacks where adversaries have full control of a number of authenticated devices and behave arbitrarily to disrupt the network are referred to as Byzantine attacks [3].Once the active set of insider nodes in the network are turned to be malicious by the attackers then the whole network will be under the control of adversaries and further secured data transmission is not possible. This is very crucial in case of mobile devices used in military fields and medical fields for transferring patient reports and medical advises. A byzantine adversary can prevent the route establishment by dropping the route request or response packets, modify the route selection metrics such as packet ids, hop counts, drops packets selectively, creates routing loops, forwards the packets through non optimal paths for time and bandwidth consuming purpose and so on[4].Are the attacks in which a single node or a set of nodes works together to create loops ,forwards packets through non optimal paths or selectively drops the packets which results in disruption or degradation of the routing services and network performance.

According to Jetcheva and Johnson ,insider attacks are also known as Byzantine [5] attacks and the protocols which are able to afford service in the presence of byzantine nodes are known as Byzantine resilient protocols.“Byzantine problem” is the term that refers to the circumstances where a few defective/corrupted members of the group acts in an arbitrary way and cause a system malfunction [6]. This kind of problem was first stated by L. Lamport [7] as "Byzantine General Problem”.

Certain features of byzantine attacks are common like "selfish" node problem [8] like not forwarding the received data packets, but the intension of both are quite different. The aim of the selfish node is to take part in the routing and in the network without spending its own resources while; the aim of the byzantine node is to interrupt the communication of other nodes in the network, without considering its own resource utilization.

Black hole or sinkhole attacks, Byzantine wormhole attacks, Byzantine Overlay network wormhole attacks, gray hole attacks, flood rushing attacks and selfish node attacks are the various kinds of byzantine attacks in adhoc networks and are explained below in detail.

### *4.1 Black hole or sink hole attacks :*

Black hole attack is a rudimentary type of byzantine attack. In this type of attack the adversary selectively drops the packets, modifies certain packets and forwards most of the data in its original form, from time to time stops forwarding packets received by it but still actively participates in routing. While the adversary is selected to be a part of routing path, it stops the communication through that path by stopping forwarding activity [9-10]. Also it sends bogus routing information to the source node alike Route Reply (RREP) message with fake destination sequence number. Thus the source node may think it is having fresh path to the destination and sends packets through the new route. So when it is being selected to be in the path, it may simply discard or exploit the data. This kind of attack is extremely undetectable by its monitoring nodes and thus difficult to predict or eliminate.

### *4.2 Byzantine Wormhole attacks:*

Wormhole attack is one of the most serious attacks in Manets. In this kind of attack a set of malicious nodes forms a tunnel amongst them and passes the packets between them without other nodes notice [10-11]. If the adversaries are present near to the source and destination then higher the risk. If the source node sends a route request RREQ to the destination D through the nearby adversary, then it will be tunneled and send directly to the partner adversary present near to the destination. Thus before the other route details reaches the destination node the route that involves the adversaries reaches D faster and thus that will be selected by D to unicast the RREP to the When the adversaries are selected to participate in the route and receives the data from S ,it stars the attacks using black hole attack.

### *4.3 Byzantine Overlay Network Wormhole Attack :*

This sort of attack is the most serious one and is common when more number of nodes in the network turn to be malicious in nature and become neighbors to the routing protocol. Whereas Byzantine Wormhole attack is more common while few nodes turn to be malicious. Since the packets are tunneled over the overlay network, the routing protocol considers/assumes the adversaries as their reliable neighbors and selects them to participate in routing.

### *4.4 Gray hole attacks :*

In this type of attack the adversary node advertises itself have a valid route to the destination and participate in the route. After being a part of the route it drops the packets that are intercepted in an unpredictable manner[12]. Sometimes it forwards the packets from/to a specific set of nodes properly and later it may selectively drop the packets from the same. This type of attack is too difficult to be detected than the black hole attack where the packet drops are carried out with certainty[13]. A node which behaves maliciously may also turn to be as a normal node later and vice versa.

### *4.5 Flood Rushing attack :*

Flood rushing attack is a kind of effective denial-of -service attack. It causes serious effects especially in reactive protocols such as AODV which sends the Route Request packets (RREQs) by employing flooding concept. In this type of routing protocols flood suppression technique will be used to avoid overconsumption of network resources. When the source node floods the RREQ, usually the RREQs which reach early will be taken in to accordance and further requests will be ignored by the nodes in the routing path. The adversary nodes takes advantage of this concept and rushes to spread the RREQs throughout the network and thus it leads to insistent failure to establish the adversary free route even when authentication techniques are used. This consumes a lot of network resources such as bandwidth and battery power [14].

### *4.6 Selfish Node Attack:*

Selfish node attack is a type of attack in which the attacker denies cooperating with other nodes in routing for the reason of its energy consumption, but tries to participate in active routing by sending its own packets and dropping the packets it is supposed to forward [15].

## V. Byzantine Mitigation Mechanisms

In order to mitigate the byzantine attacks in adhoc networks, a set of security mechanisms and protocols are proposed in the recent past. Almost all the mechanisms are (i) trust based (ii) incentive based and (iii) cryptography based.

### *5.1 Trust-based approaches:*

Trust is a significant characteristic in the design and testing of secure distribution systems [16]. Moreover it is one of the main concepts that guides in decision-making and is a crucial factor in determining the relationships [17-18].

Buchegger et al [19] proposed a protocol that uses a reputation mechanism to detect the misbehaving nodes using watchdog and path rater. A trust manager estimates the level of trust of alert reports and the reputation system estimates the each node's reputation. Each node prepares a report about other nodes and the trusted nodes reports only will be processed. It is not clear how the trusted nodes turned to be as compromised nodes and the reputation systems do not provide any protection against false accusations.

A trust model proposed by Yan et al assigns trust values to all the participating nodes based on their observed behavior. The nodes that does not meet the required trust level are excluded from routing path.

A secure routing scheme for MANET proposed by Li and Shanghal [20] assigns quantitative trust values to the nodes based on the recommendation of the other nodes and observed behavior pattern. It excludes the malicious nodes to participate in routing path. But there is a chance that the malicious nodes can drop the trust query messages intentionally, and in that case the scheme will be ineffective.

Security-aware ad hoc routing (SAR) proposed by Yi et al [21] groups nodes based on their trust level. Secret group key is shared among the nodes of same category. During the route discovery ,the source node S can specify the least security prerequisite of a node to participate in the routing path. S can impose the requirement by encrypting the RREQ packet with the shared key. The major problem of this approach is the likelihood of malicious nodes to take over the nodes with high security classifications in order to gain access to the secret group keys.

Buchegger et al [22] proposed a protocol named CONFIDANT based on popular watchdog and pathrider concepts. It is a Baysian theorem based reputation mechanism to determine the degree of reputation possessed by every node in the adhoc network In this approach, malicious nodes are barred from forwarding the route replies as well as sending their own route request. The trust levels of alert reports are evaluated by a trust manager and in addition a reputation system rates each node. Nodes process only the trusted reports.But,it is not mentioned clearly about how fast the trust level of a non cooperative compromises node can be adjusted particularly if its trust value is initially high.

Zouridaki et al proposed a novel frame work [23] to determine the reliability of data packets in the adhoc networks data exchange. First and second and information collected from the neighbor nodes is used to determine the reliability of a node. Opinion metric is used to detect the maliciousness of a node. Confidence and trust limits have been used by the authors to predict the data delivery statistically.

Nasser et al's system [24] identifies the malicious nodes which can lead to network partition .The proposed approach uses an enhanced intrusion detection system namely ExWatchdog that overcomes the problem of self overhearing by watchdog mechanism.

### *5.2 Incentive-based schemes:*

Zhong, Chen and Yang[25] offered an Incentive-based Simple, Cheat-Proof, Credit-Based System namely Sprite for MANETs. Nodes are provided incentives to cooperate and report about its neighbor nodes to a centralized entity called CCS honestly. This proposal requires on line access to an entity called Credit Clearance Service (CCS) for its functioning. This may not be always possible for purely adhoc network MANET.

Ghosh et al improved the trust management to provide security against malicious nodes that works together. Their distributed method has taken confidence level of trust in to account for calculating the trust value to mitigate the selfish nodes from the network. Number of forwarded packets metric is taken into consideration by direct observation to determine the trust worthiness of the nodes. Black hole, Gray hole, false accusation and DoS attacks have been considered [26].

### *5.3 Cryptography Based:*

Conventional authentication and encryption mechanisms are based on cryptography which is preventive mechanisms. HongMei et al [27] argues that cryptography, Hash functions and digital signatures cannot defend attacks from compromised insider nodes such as black hole attacks since the compromised nodes too create valid signatures. Further Crescenzo et al [6] argues that using cryptography-based tools is not sufficient to attain Byzantine adversary free network.

Secure Data Transmission (SDT) protocol avoids black hole attacks by using authenticated end-to-end acknowledgments. In this approach the destination node sends back an acknowledgement as a proof of packet receiving[28].This scheme is able to detect only the black hole attack and is incapable of determining the adversarial nodes along the routing path.

Sanzgiri et al [29] provided an end to end authentication for AODV and DSR protocols using digital signatures. Minimum path selection is also offered by them using onion technique, where each node in the routing path performs and accumulates digital signatures and public cryptography encryption/decryption. The destination node strips off the encryption/signed layers to determine the path. It is quite expensive.

Zhou and Haas [30]used threshold cryptography to realize the key management system to provide a multipath protocol .Few nodes plays role as servers and an authority is used to initialize the servers. Zapata and Asokan [31] propose Secure AODV (**SAODV**) that uses hash chains and digital signatures to secure routing messages.

### *5.4 Analytical Approaches:*

Fei Xing and Wenye Wang [32] used an analytical approach to estimate the survivability of the network in misbehaving and failure nodes existence. They classified the mobile nodes in the adhoc network into four categories namely (i)cooperative node,(ii)malicious node,(iii)byzantine node and (iv)failure node based on reliability coefficients. A special kind of counter called Nuglet counter is used to estimate the probability of misbehavior f a node at a time instant. This strategy helps in deriving the network survivability based on network characteristics and node behavior investigation.

Alavaro A. Cardenas et al., [33] suggested a byzantine mitigation mechanism for adhoc networks based on Sequential Probability Ratio Test(SPRT)including a quantitative approach called DOMINO. The authors implemented a two step process for identifying byzantine behavior of a mobile node. First ,the transition probability of mobile nodes that are presently in direct communication were calculated. In the second step, Markov chain was estimated for each mobile node with transition probability p and 1-p.Misbehaving nodes are detected by observing the state alterations through Markov chain. Finally, the identification of misbehaving mobile nodes was carried out by monitor the state changes through Markov chain.

Two reactive methods has been proposed by Neeraj Jaggi et al.,[34]to mitigate the byzantine activities in Manets.An analytical non adoptive approach is used to mitigate the hostile misconduct of mobile nodes. While the subsequent approach is the distributed approach that enables dynamic response of genuine mobile nodes in the network. State probabilities and transmission probabilities are determined using Markov analysis.

Byzantine nodes in an adhoc network are detected by using a Collaborative watchdog method by Hernandez-orallo et al., [35]. Poisson distribution is incorporated to analyze the cooperation between the mobile nodes and define the two states of nodes namely NOINFO and POSITIVE states. Continuous

Time Markov chain (CTMC) is incorporated for network modeling and the network is estimated using watchdog mechanism. The time and cost to detect the byzantine nodes is estimated with the support of watchdogs.

Geetha, A., and Sreenath, N., [36] estimated the reputation level of each mobile node in the Manet based on Cronbach Alpha based Mitigation coefficient (CAMC) to ensure the cooperation among the mobile nodes. It is a distributed twofold approach in which the variance and standard deviation probability of successful data delivery is estimated in the first stage .Further the authors have calculated Cronbach Alpha based Mitigation Coefficient(CAMC- $\alpha$)to determine whether a node is byzantine or not. Based on the value of $\alpha$ ($\alpha$ <0.4), the byzantine nodes are identified and are isolated. The proposed method outperforms the well known CONFIDANT and PCMA protocols.

## VI. Metrics To Analyse The Performance Losses By Byzantine Attacks

Due to byzantine attacks the adhoc networks survivability affected a lot, almost all of the researchers analysed the effects in terms of throughput, packet delivery ratio, packet drop rate, and total overhead metrics that helps in determining the network performance.

*Packet delivery ratio*: The ratio between the number of packets received by the destination node to the number of packets sent to the destination node.

*Throughput:* The total number of packets successfully delivered to the destination in a specified instant of time.

*Packet drop rate:* The total number of data packets dropped during the data transmission process.

*Total Overhead:*Rattio of the sum of data packets and control packets to the number of data packets forwarded by a mobile node.

*Control Overhead:* The maximum number of bytes of control packets delivered to the destination at a point of time

## VII. Conclusion

In this paper, detailed analysis about byzantine attacks, its types and the various categories of mitigation mechanisms to overcome it are carried out. It is obvious that byzantine attacks are highly crucial to detect and the activities carried out by the byzantine nodes are very hard to predict and avoid by conventional cryptography mechanisms. They are the attacks by active insiders that have enough authentication to participate in active routing process of the ad hoc networks. The cryptography ,trust based mechanisms and incentive based mechanisms all are need to exchange lot of messages to ensure authenticity ,that consumes lot of power and bandwidth which are highly crucial in Mobile ad hoc networks .Whereas the stated distributed mathematical models consumes comparatively less resources of the network and also ensures high cooperation among the nodes and reliable data communication.

## References

[1] Baruch Awerbuch , Reza Curtmola , David Holmer , Cristina Nita-Rotaru , Herbert Rubens, ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks, ACM Transactions on Information and System Security (TISSEC), v.10 n.4, p.1-35, January 2008 [doi>10.1145/1284680.1341892] http://dx.doi.org/10.1145/1284680.1341892

[2] Geetha,A and Sreenath,N.,"Review of Security Threats and its Countermeasures in Mobile Adhoc Networks," Advances in Natural and Applied Sciences, Vol 9,no 6, P 421-425 ,2015.

[3] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "On the survivability of routing protocols in ad hoc wireless networks," in Proc. of SecureComm'05. IEEE, 2005. http://dx.doi.org/10.1109/securecomm.2005.30

[4] R. Curtmola and C. Nita-Rotaru,"BSMR:Byzantine- Resilient Secure Multicast Routing in Multi-Hop Wireless Networks,"Proc.Fourth Ann. IEEE Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON '07), 2007

[5] J. G. Jetcheva and D. B. Johnson, "Adaptive demand-driven multicast routing in multi-hop wireless ad hoc networks." in Proc. Of MobiHoc, 2001, pp. 3344

[6] Crescenzo, G. D.,Ge, R., & Arce, G. R. ( FEBRUARY 2006). Securing Reliable Server Pooling in MANET. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS* ., Vol 24,no 2,pp357-369.

[7] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Languages Syst.*, vol. 4, no. 3, pp.382–401, Jul. 1982 http://dx.doi.org/10.1145/357172.357176

[8] P. Kyasanur and N. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks," in *International Conference on Dependable Systems and Networks (DSN'03)*, 2003. http://dx.doi.org/10.1109/dsn.2003.1209928

[9] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[10] Th. Clausen et al., "Optimized Link State Routing Protocol," IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003.

[11] "CSI/FBI computer crime and security survey," CSI Computer Security Institute, vol. 8, 2003.

[12] Sen J. ,Chandra M. ,Harisha S. G. ,Reddy H. ,Balmuralidhar P. , "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", Information, Communications and Signal Processing ,2007,6th International IEEE Conference. http://dx.doi.org/10.1109/icics.2007.4449664

[13] H. Deng, H. Li, and D.P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, Vol. 40, No. 10, October 2002.

[14] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Rushing attacks and defense in wireless adhocnetwork routing protocols, In Proceeding of theACM workshop on Wireless Security WISE 2003,San Diego, CA, USA, September 19, 2003, pp. 1-11. http://dx.doi.org/10.1145/941311.941317

[15] Panagiotis Papadimitratos and Zygmunt J. Haas. Secure Routing for Mobile Ad hoc Networks. In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 2002

[16] Z. Yan, P. Zhang, and T. Virtanen. Trust evaluation based security solution in ad hoc networks. In Proceedings of the 7th Nordic Workshop on Secure IT Systems (NordSec 2003), October 2003

[17] Shillo, M.; Funk, P.; Rovatsos, M. Using trust for detecting deceitful agents in artificial societies. Applied Artificial Intelligence, vol.14, no.8, p.825-48 Sept. 2000. http://dx.doi.org/10.1080/08839510050127579

[18] Warne, D., Holland, C.P. Exploring trust in flexible working using a new model. BT Technology Journal, vol.17, no.1, p.111-19. Jan 1999 http://dx.doi.org/10.1023/A:1009683126828

[19] S. Buchegger and J-Y.L. Boudec, "Performance analysis of the CONFIDANT protocol", In Proceedings of the 3rd ACM Symposium on Mobile Ad Hoc Networking and Computing, pp. 226-236, 2002. http://dx.doi.org/10.1145/513800.513828

[20] H. Li and M. Singhal. A secure routing protocol for wireless ad hoc networks. In Proceeding of the 39th Hawaii International Conference on Systems Science (HICSS-39 2006), pages 225–234, January 2006

[21] S. Yi, P. Naldurg, and R. Kravets. Integrating quality of protection into ad hoc routing protocols. In Proceedings of the 6th World Multi-Conference on

Systemics, Cybernetics and Informatics (SCI 2002), pages 286–292, August 2002.

[22] S. Buchegger and J-Y.L. Boudec, "Performance analysis of the CONFIDANT protocol", In Proceedings of the 3rd ACM Symposium on Mobile Ad Hoc Networking and Computing, pp. 226-236, 2002. http://dx.doi.org/10.1145/513800.513828

[23] Zouridaki C,Mark BL,Hejmo M,Thomas RK.A quantitative trust establishment framework for reliable data packet delivery in MANETs.In:Proc,of 3r ACM workshop on security of adhoc and sensor networks,vol .1,no.1,p.1-10.2009.

[24] Nasser, N.; Yunfeng Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks", IEEE International Conference on Communications, ICC apos; Vol-07 , Issue 24-28 June 2007 , pp.1154 – 1159. http://dx.doi.org/10.1109/icc.2007.196

[25] S. Zhong, J. Chen, and Y. Yang. Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks. In Proceedings of IEEE INFOCOM, pages 1987– 1997 Vol.3, March 2003. http://dx.doi.org/10.1109/infcom.2003.1209220

[26] T. Ghosh, N. Pissinou, and K. Makki, "Towards Designing a Trust Routing Solution in Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 10, pp. 985-995, 2005. http://dx.doi.org/10.1007/s11036-005-4454-4 http://web.cse.msstate.edu/~ramkumar/p985-ghosh.pdf

[27] HongMei Deng, Wei Li, Dharma P. Agrawal. Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine, October 2002, p70-75. http://dx.doi.org/10.1109/MCOM.2002.1039859

[28] P. Papadimitratos and Z. Haas, "Secure data transmission in mobile ad hoc networks," in 2nd ACM Workshop on Wireless Security (WiSe), 2003. http://dx.doi.org/10.1145/941311.941318

[29] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in 10th IEEE International Conference on Network Protocols (ICNP'02), November 2002. http://dx.doi.org/10.1109/icnp.2002.1181388

[30] L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network, 13(6):24–30, 1999 http://dx.doi.org/10.1109/65.806983

[31] M. G. Zapata and N. Asokan. Securing ad hoc routing protocols. In WiSE '02: Proceedings of the ACM workshop on Wireless security. ACM Press, 2002. http://dx.doi.org/10.1145/570681.570682

[32] Fei Xing Wenye Wang, Modeling and Analysis of Connectivity in Mobile Ad Hoc Networks with Misbehaving Nodes. in prod., of IEEE International Conference on Communications, Vol. 4, No.3, pp.1879– 1884, (2006).

[33] Alvaro A., C´ardenas, Svetlana Radosavac and John Baras, S., Evaluation of Detection Algorithms for MAC Layer Misbehavior: Theory and Experiments. IEEE Transactions on Networking,Vol. 17, No. 2, pp.605-617, (2009). http://dx.doi.org/10.1109/TNET.2008.926510

[34] Neeraj Jaggi, Vamshikrishna Reddy Giri and Vinod Namboodiri. Distributed Reaction Mechanisms to Prevent Byzantine Misbehavior in Wireless Ad Hoc Networks. in proc of the Global Communications Conference, GLOBECOM 2011, Houston, Texas, USA. IEEE, Vol. 1, No. 1, pp. 1-6, (2011).

[35] Hernandez-Orallo, E.,Serraty, M.D., Cano, J-C., Calafate, T.and Manzoni, P. Improving byzantine node detection in MANETs using a collaborative watchdog. IEEE Letters. Vol. 16, No. 5, pp. 642-645, (2012). http://dx.doi.org/10.1109/LCOMM.2012.030912.112482

[36] Geetha,A and Sreenath,N., "Cohen Kappa Reliability Coefficient Based Mitigation Mechanism For Byzantine Attack In Manets". International Journal of Applied Engineering
Research, Vol 10,No 9,pp. 23989-24001,(2015).

A.Geetha has completed her M.E degree from the Department of Computer Science and Engineering, at Anna University June 2006.Currently she is pursuing a Doctoral Degree in the Department of Computer Science and Engineering at Pondicherry Engineering College, Pillaichavady, Puducherry, 605014,India. Her research interests are in the area of Wireless Mobile Adhoc Networks, specifically routing, Byzantine attacks detection/avoidance and network security. She is having more than 18 years of teaching experience.

Sreenath Niladhurai received his M.Tech from University of Hyderabad and Ph.D. in Computer science and Engineering (2003) from IIT Madras, India. He has been working at Pondicherry Engineering College since then and currently he is a Professor in the Department of Computer Science and Engineering and Dean, Autonomy and Accreditation at Pondicherry Engineering College, Pillaichavady, Puducherry –605014.He has co-authored 2 books and over 50 journal and conference papers. His research areas are high speed networks, Network Security and Optical Networks