Enhanced routing for secured ad-hoc network

U. Kumaran[1], A. Ramachandran[2], J. Jegan[3], E. K. Subramanian[4]
[1]Department of CSE, Mother Theresa Institute of Engineering and Technology, Chittoor, India
[2]B. S. Abdur Rahman Crescent Institute of Science and Technology Chennai, India
[3]Sreenivasa Institute of Technology and Management studies, Chitoor, India
[4]Saveetha School of Engineering, Chennai, India

Article Info

Article history:

Received Dec 2, 2019
Revised Feb 4, 2020
Accepted Feb 18, 2020

Keywords:

Authentication
Mobile ad-hoc network
Reliability
Security attacks
Vulnerability

ABSTRACT

A self-configured network forming an arbitrary topology of mobile routers through wireless connection is commonly referred as MANET (mobile ad-hoc network). Random movement of routers allows the network to organize arbitrarily hence rapid unpredictable changes may occur in the topology of the wireless network. When there is no possibility of setting up permanent networks, MANETs are set up for carrying out the operations temporarily. As there is no fixed frame for this system, usage of available resources for reliable communication is a great challenge for MANETs. The nodes participating in packet routing in ad-hoc networks faces security issues such as maintaining the confidentiality of the packets, integration, availability of the network to meet the traffic, requirement of authentication for reliable data communication etc. Dropping of packets maliciously in an attack is known as black hole attack.An attempt is made in this paper to detect dynamically using the security of cross layer called as honeypot and classify the mechanisms to understand the strengths & threats of the protocols used for routing to suggest a concrete solution for the problems related to the mobile ad-hoc networks. The methodology of honeypot detects and isolates the attacks of the black hole. The results prove better delivery of packets with decreased load of the network.

Corresponding Author:

Dr. U. Kumaran,
Department of CSE,
Mother Theresa Institute of Engineering And Technology,
Chittoor, Andhra Pradesh, India.
Email: drkumaran04@gmail.com

1. INTRODUCTION

Mobile host utilize ad-hoc networks as one of the new standard of wireless communication. It does not require any solid infrastructure for routing like mobile base stations. Direct communication occurs between nodes that are within their frequency range to relay messages that are far apart but connected through wireless links. Frequent changes occur in the topology of the network due to the mobility of the node. Problems related to security arise due to lack of network infrastructure and communication through wireless links [1]. Solving the security problem of MANET is possible within a single layer hence the performance enhancing can be done using cross layer design exchanging information in between layers. Dependence between layers is exploited increasing the performance where the cross layer design shares information on state of one layer with that of other layers.

The layers of the network suffer from attack of black hole which acts as a threat against the protocol used for routing in MANET which is done by packet dropping. The aim of such attacks is downgrading the network communication or to make the destination node unapproachable. Detection of such black hole nodes is done by monitoring of lost traffic. All the packets are dropped in the path of communication by the black hole attacks. Implementation of technique of cross layer security, secures a MANET from the attack of black hole problem. It is crucial to transmit information from the sender to the receiver reliably through the mobile nodes as all the nodes receive the data packets within the range of the source node. Also the receiver node can go out of the range anytime as all the nodes are mobile and none are fixed. Hence in the absence of a fixed infrastructure communication through mobile wireless links is the basis of MANETs.

Ad-hoc networks are susceptible for threats due to the usage of wireless links which leads to message distortion. High probability of error is possible due to poor protection of the mobile nodes hence attacks may not only due to mobility but can also within the node which has to be taken into consideration. The proposed method involves security solution based on honeypot which indicates the importance of learning the probing method of the attackers who attempt to access the MANET network. Precise data is given by the honeypot where only scare amount of data contains activity with malicious nature. Detection of black hole attack is implemented by the proposed method which isolates in MANET consisting of the honeypot which can anomaly detect the black hole using the cross layer security method which uses the attack features against the network and MAC layer.

In this technique feedback from lower layer is sent to the feedback from upper layer, where the feedback from lower layer indicates the data collected from MAC layer and the feedback from upper layer indicates the data obtained from network layer. This concept is implemented by the proposed algorithm of monitoring of data from cross layer which computes the overload of network attack by counting the network layer's missed IP and the number of packet drop from MAC layer. Estimation of overhead of the network attacks is done by the algorithm of dynamic timer. Hence the design of cross layer technique isolates the black holes from the MANET using the network layer and MAC layer. These isolated nodes with black holes are updated in the routing table which is broadcasted throughout the network.

2. BACKGROUND

MANET's network layer is susceptible to various attacks leading to routing attacks. Several methods are implemented to solve such problem commonly known as black hole attack. A distributed mechanism which detects the attacks in MANET collaboratively is discussed in conventional methods. This methods involves four stages namely collection of local data, detection at local network, detection at co-operative network and detection at global network. The collection of data at local level consists of estimating table containing the data about malicious nodes. The phase of local detection detects the network node with black hole. If the inspection result is obtained as positive then the node is detected as normal node else the process of detection is started by the node of initial detection which is notified to all the neighboring nodes in the process of detection while a reaction in global network is warned about the attack throughout the network.

Basic features of MANETs are

a. Self management& organization
b. Mobile nodes
c. Frequent variation in topology of network
d. Communication through wireless links
e. Same node acts as router, source and destination
f. Routing through multi-hopping technique
g. Limitation in power
h. Scale variability
i. No centralized control
j. Dynamic network topology
k. Operation is distributed
l. Does not require any access point

Field of application of MANETs is as follows:

a. Wireless sensor network
b. Medical field
c. PAN (Personal Area Network)
d. Military field
e. Business sector

2.1. Wireless networks-types

The network topology where each node is able to connect with all other nodes without the requirement of any protocol to take over the routing process is the conventional radio relay where the range is considerably big is the first kind. The second type is the radio relay with smaller range such that each node cannot get connected to all the nodes instead makes use of the nearby nodes to reach the far away nodes with the neighboring nodes acting as routers. This paper focuses the security issues of the second type in routing the data packets.

The mechanism for security is the essential sets that are encapsulated with any routing protocol. Issues such as preventing, detecting and proper response to the security attacks are taken care by the security mechanisms. For a secure and reliable ad-hoc network as shown in Figure 1, five important security goals are to be considered for proper communication and to maintain the confidentiality. Data deletion, including error messages, imitation of node are the attack possible in the ad-hoc networks. Existing techniques for the above issues are not able to meet the requirements to provide reliable communication. Hence the proposed work integrated in the design phase of the routing protocol acts as a feasible solution for the ad-hoc networks security needs.

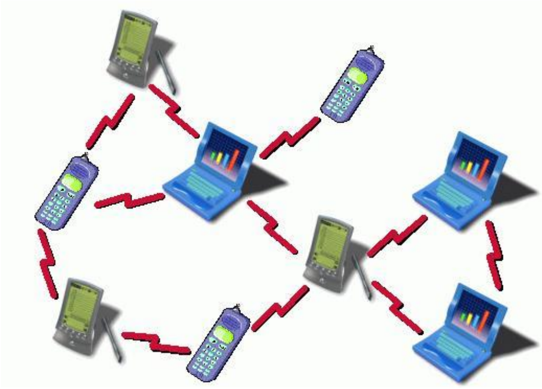

Figure 1. MANET (mobile ad-hoc network)

3. PROBLEM STATEMENT

The issue related to the security of protocols of routing is the problem focused in this paper. Dynamic topology of the mobile ad-hoc network is the reason for not able to provide protection from the malicious attackers. The existing mobile ad-hoc networks are under the threat of vulnerable attacks under various fields of application and the corresponding solutions are valuated [2]. Informal exchange of network topology of routers is established between nodes and the targets in order to avoid the malicious attacks reducing the efficiency of network communication. Congestion can be caused resulting in service denial due to erroneous information to the routers injected by the external attackers, distorted or old router information which in turn overloads the network through retransmissions.

Detection and correction are harder for the nodes that have internal compromise. Valid signatures generated by the private keys of the nodes under compromise will not work as the information for routing at each node. The topology of ad-hoc network is dynamic which makes the detection of nodes under compromise difficult using routing information. Mobile ad-hoc networks rely on relay packets instead of infrastructure of the routing. Hence proper communication in mobile ad-hoc network is possible between the nodes only through cooperation and packet forwarding. When individual nodes are considered it is good not to cooperate ad power is saved and less vulnerable to the security attacks. This paper discusses the possible vulnerabilities with their prevention and detection mechanisms for those attacks.

3.1. Problems of black hole attacks

The protocol of AODV is used by the node with malicious black hole for advertising it having the node’s shortest path with its packets to be intercepted. Therefore the reply from the malicious node is sent to the source node even before the actual node sends the reply creating a forged route. Then the malicious node chooses either packet dropping for DoS attack or using its location in the route for the attack of man in the middle. The rules of the AODV protocol are violated by the node of Black hole as it sends fake message incrementing the field of hop count as one by setting the IP address of the source to an IP address that does not exist or unicast the fake message to the source. As the fake message reaches the source the route is updated through the attack node to the destination node. The challenge is to detect the black hole due to the dynamics of network of MANET and to proceed with malicious node isolation from communicating. Hence there is requirement of novel secured routing method for packet delivery from source to destination nodes.

4. NEED FOR SECURING MOBILE AD-HOC NETWORK

The techniques existing for securing MANET includes detection of intrusion and secured routing technique.

A. *Detection of Intrusion*. The significant part of the security system is the detection of intrusion which detects the security policy violation by the activities of the monitoring system to remove unwanted disturbances. Immediate response is initiated by the system once there is detection of an attack as shown in Figure 2 in order to avoid any damage to the system [3]. Following are the techniques to detect the intrusions in MANET.

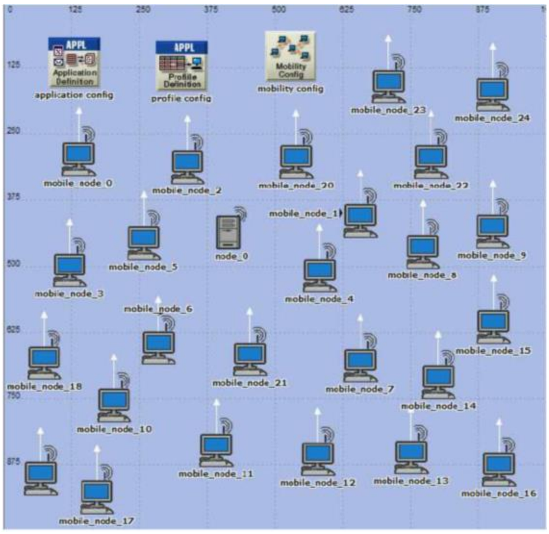

Figure 2. Topology of the network with 25 mobile nodes & an intruder node

B. *Detection of intrusion based on misuse*. Signatures are attacked by the misused based detection of intrusion in the activities of the current system. Generally commercial detection of intrusion prefers this type as very low false rate is provided and is very efficient. But they are not able to detect fresh attacks which require database updating frequently as system is efficient as that of the signature database [4].

C. *Detection of intrusion based on anomaly*. Any deviations from the normal patterns are detected by this type of intrusion based on anomaly. Unknown attacks are detected and possibility for detection of normal activities as anomalies is high.

D. *Detection of intrusion based on specification*. Detection of modification and fake attacks is done by this technique but identification of attacks that does not break directly the specifications of the protocol is not possible with this technique.

E. *Security based routing*. In mobile ad hoc network various types of attacks are there for the routing layer. Complicated attacks such as Rush attacks & Wormhole attacks are difficult to detect. Following are the types of security based routing.

F. *Pathrater & watchdog*.The performance of MANET is expanded by pathrater and watchdog even in the presence of misbehaving nodes. Watchdog stores the packets in the buffer that are to be forwarded in order to identify the misbehavior [5]. Watchdog sneaks in order to decide whether the packets are forwarded by the neighboring node without any alteration. The packets are discarded if the sneaked packets match the packets in the node buffer however packets are considered to be altered if they stay beyond a period in the buffer finding no match [6]. The packet forwarding node is considered to be suspicious. If the total number of violations crosses predetermined threshold the node is considered to be malicious. This malicious node is just passed on to the path rater for evaluation. In a particular network all the node are rated by the path rater separately. From the perspective of each node, ratings are updated. During forwarding the packets, unbiased rated node gets altered depending on the observed behavior. An immediate rating of-100 is given to the misbehaved nodes observed by the watchdog [7]. Hence packet modification/mishandling are related to misbehavior whereas link breaks are related to unreliable behavior.

G. *Communities with localized self- healing security based routing*. Packet forwarding mainly relies on neighboring nodes through wireless links is the basis of community with self healing [8]. At each step of packet forwarding community based routing involves redundancy such that each conventional node is converted to community based node [9]. At least one good node is required in the community which is of cooperative nature for the self healing community to be purposeful. Specific attacks disturbing the ad-hoc network are dealt by the good nodes providing solution to defend those attacks.

5. GOALS OF SECURED MANET

There are some manet purposes which are guaranteed:

A. *Authentication.* A node in the network must not be imitated as it is crucial to identify the secured node through encryption of their respective codes. Impersonated nodes can hack resources that are confidential and can spread vulnerable data in the network.

B. *Continual service.* The designated service of the node must be provided and should avoid service denial. Possibility is their where some of the network services are made unavailable by some selfish nodes.

C. *Integration.* Guaranteed identification of the sender is the process referred as integration. Two possible attacks are accidental attacks and malicious attack which is classified based on their intension [10, 11]. Accidental attacks are due to alteration that happens unintentionally, whereas malicious attack is an intentional alteration.

D. Privacy. Accessing data only by authenticated persons is considered as privacy which is maintained confidential. Others without special permissions are not allowed to access the data.

E. *Authority.* For assigning authority to users, the access rights are given at various levels which undergo the process of authorization. Users who possess the credentials are only allowed to access the resources [12].

F. *Ambiguity*. The sender of the data packet can be identified using this information. This data has to be maintained confidentially by the user and should not distribute it. It is similar to preserving the privacy.

6. IMPLEMENTATION OF PROPOSED METHOD

6.1. Architecture of proposed method

The proposed method of honey pot cross layer design uses the data from the cross layer which is collected from MAC layer and network layer. Additionally security is provided by the concept of honey pot. The architecture of the proposed algorithm is shown in Figure 3 which consists of the following modules namely detection layer in the malicious node [13, 14], Network layer and MAC layer with the route lookup and Network layer & MAC layer’s isolation.

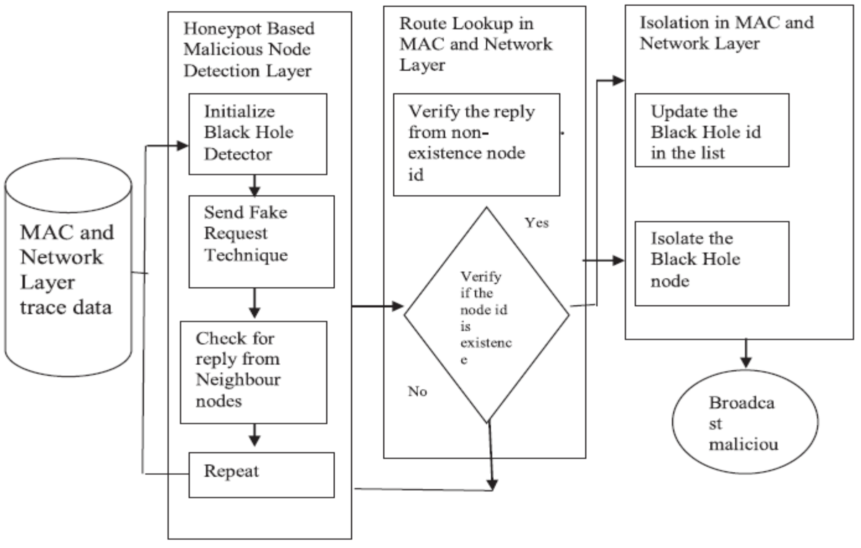
MAC and Network Layer trace data
Honeypot Based Malicious Node Detection Layer
Initialize Black Hole Detector
Send Fake Request Technique
Check for reply from Neighbour nodes
Repeat
Route Lookup in MAC and Network Layer
Verify the reply from non-existence node id
Verify if the node id is existenc e
Yes
No
Isolation in MAC and Network Layer
Update the Black Hole id in the list
Isolate the Black Hole node
Broadca st maliciou

Figure 3. Architecture of the proposed method

Input to the detection layer of the malicious node is obtained from the trace data of MAC layer and network layer. The packet loss of the lower layer is done by calculating the number of dropped packets in the MAC layer. DSN is used by AODV for entry of each route. Freedom of the loop is ensured by the DSN [15-17]. Each node maintains DSN which increases monotonically are involved each of the originating nodes. The information about each of the DSN is included in the route table entry of each node. Updating of DSN is done whenever new information is received from RREP about DSN. Hence it is important to measure the DSN missing for identifying the attacker black hole. Correlation of features of the network layer with that of MAC layer is done by the monitoring algorithm of cross layer data. The attack load is calculated by this algorithm by the calculation of the above features. Therefore the network load is determined by this algorithm which depends on the features of the MAC and routing layer.

6.3. Network and MAC layer's route lookup

The detection process is invoked dynamically by the route lookup in the network layer and the MAC layer (cross layer) which is based on attack load. Increasing of attack load indicates the starting of the detection process by the technique of dynamic timer.

6.4. Network layer & MAC layer's isolation

Isolation of the network layer and the MAC layer is done by the cross layer which isolates the malicious node which sets a flag indicating presence of malicious node. Any node which communicates with a node with a non existing id is marked as malicious node [18-22]. Both the features of single layer and cross layer are used for isolation of the malicious node. Black holes that are malicious in the network are isolated using the isolation technique based on the features of the cross layer. The detail of the malicious node is broadcasted in the network as broadcast packets [23]. Detail such as node id of the black hole is collected by the technique which is broadcasted by the network to the other nodes. The isolation module provides the node id of the malicious node as the input represented as RTF id which indicates the id flag of the malicious node and detection flag, as both are set the id of such node is broadcasted in the network.

7. RESULTS & DISCUSSION

The proposed solution meets the security threats of MANET namely tapping, behavior of the intruder, integrity etc [24]. Impersonating mobile nodes is easier in MANET to start an attack due to intruder. In order to avoid the attacks of intruder the proposed mechanism analyses the network with and without an intruder where there is risk of data integrity hence establishing a reliable relation among mobile nodes is possible by higher degree of trust by the implementation of intruder behavior. Every time the network detects the intruder, all the routes through it will be reallocated. Once the intruder is detected trying to damage the network, application traffic is completely blocked at that mobile node [25]. Hence there are zero bytes sent or received through the intruder as shown in Figure 4. In the network the node 16 before the intruder has activity related to traffic sent and traffic received as shown in Figure 5 where the simulation is done until 2 hours.

Based on the results the intruder is analyzed in the MANET network where the network traffic is checked with the intruder and without the intruder with the possible risk of data integrity. The methodology of handshaking is implemented for developing trust among the mobile nodes without any malicious attacks and leakage of information. Once after the detection of intruder all the traffic through the defective mobile node is re-routed to other trustworthy nodes hence there is nil traffic through such intruder nodes. The black hole attacks are analyzed by performance metrics such as packet delivery fraction which indicates the number of packets transmitted by the source node to the end destination node. Information of the network load is indicated by the normalized routing load. If it increases it indicates that the load in the network is increased by generation of control packets. Success of the proposed method is indicated by end to end delay. Loss of packet in the network is indicated by the packet drop ratio. The packet delivery ratio for three different networks are compared as shown in Figure 6 and the end to end delay for the same networks are compared as shown in Figure 7.

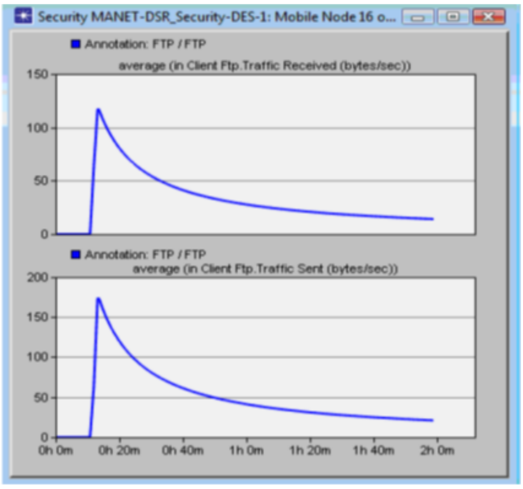

Figure 4. Sent & received traffic at intruder

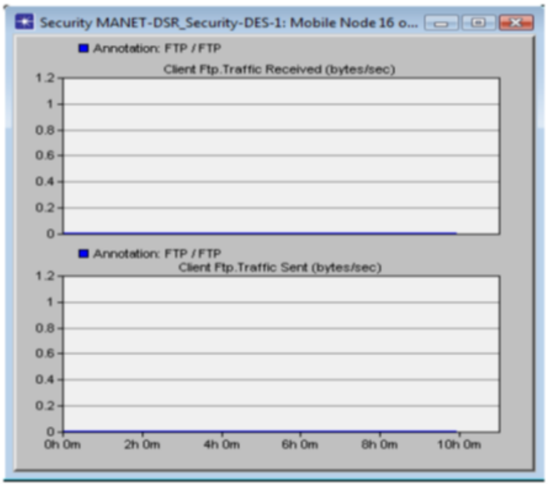

Figure 5. Sent & received traffic before intruder

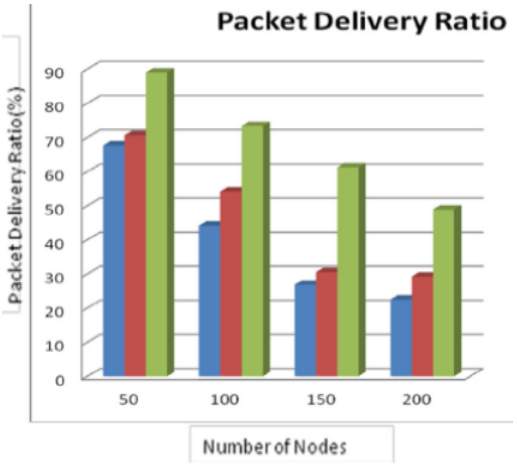

Figure 6. Comparison of packet delivery ratio

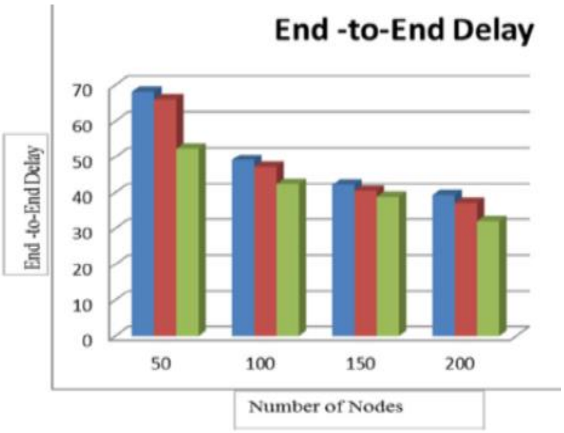

Figure 7. Comparison of end to end delay

8. CONCLUSION & FUTURE WORK

The proposed work detects the presence of black holes and performs isolation of such nodes from the network. The generation of packets by the honeypot does not involve in overloading of the network as there is no original data. The packet delivery fraction for the proposed method is 25% more than the existing methods. The normalized routing load is less comparatively which in turn reduces the network load which in turn reduces the end to end delay in the network using the proposed technique.

Selection of suitable routing protocol for MANET is the best solution to avoid the attacks of the intruders. Based on the number of mobile nodes and the traffic handled by these nodes plays an important role in selecting the routing protocol. In this paper the intruder are detected and totally isolated from the activities of the network. Further research can be carried out in exploring improved detection techniques for the intruders which are multidimensional with less computation and higher strength of security.

REFERENCES

[1] L. Zhou and Z. Haas, “Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24-30, 1999.

[2] Sergio Marti and T. J.Giuli and Kevin Lai and Mary Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 255-265, 2000.

[3] Jim Parker, Anand Patwardhan, and Anupam Joshi, “Cross-layer analysis for detecting wireless misbehavior," *CCNC 2006. 2006 3rd IEEE Consumer Communications and Networking Conference, 2006,* Las Vegas, NV, USA, pp. 6-9, 2006.

[4] IEEE Std. 802.11, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” *IEEE Std. 802.11*, 1997.

[5] D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” *Mobile Computing*, vol. 353, pp. 153-181, 1996.

[6] B. Schneier, “Secret and Lies: Digital Security in a Networked World,” *Wiley*, 2000.

[7] C. Perkins and E Royer, “Ad Hoc On-Demand Distance Vector Routing,” *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, USA, pp. 90-100, 1999.

[8] Shuyao Yu, Youkun Zhang, Chuck Song and Kai Chen, “A security architecture for Mobile Ad Hoc Networks”, Available: http://blrc.edu.cn/blrcweb/publication/ kc2.pdf.

[9] Panagiotis Papadimitraos and Zygmunt J. Hass, “Securing Routing for Mobile Ad Hoc Networks,” In *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, San Antonio, TX, 2002.

[10] J. Liu, F. Fu, J. Xiao, and Y. Lu, “Secure Routing for Mobile Ad Hoc Networks,” *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007),* Qingdao, pp. 314-318, 2007.

[11] L. Abusalah, A. Khokhar, and M. Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols,” *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 78-93, 2008.

[12] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu And And Lixia Zhang, ”Security in mobile ad hoc networks: Challenges and solutions”, IEEE Wireless Communications, vol. 11, pp. 38-47, Feb, 2004.

[13] X. Su, and R.V. Boppana, “Cross check mechannism to identify malicious nodes,” *Security and communication network*, vol. 2, no. 1, pp. 45-54, 2009.

[14] F. Stajano and R. Anderson, “The Resurrecting Ducking: Security Issues for Ad-Hoc Wireless Networks,” *International Workshop on Security Protocols*, vol. 1796, pp. 172-182, 1999.

[15] Y.C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, no.1–2, pp. 21-38, 2005.

[16] M.G. Zapata, "Secure ad hoc on-demand distance vector (SAODV) routing," *Mobile Computing and Communications Review,* vol. 6, no. 3, pp. 106-107, 2002.

[17] K. Sanzgiri, B. Dahill, B. Levine, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," *10th IEEE International Conference on Network Protocols, 2002. Proceedings*, Paris, France, pp. 78-87, 2002.

[18] F. Kargl, A. Geiß, S. Schlott, and M. Weber, "Secure dynamic sourcerouting*," Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, Big Island, HI, USA, pp. 320c-320c, 2005.

[19] W. Huang, Y. Xiong, and D. Chen, "DAAODV: A Secure Ad-hoc Routing Protocol based on Direct Anonymous Attestation," *2009 International Conference on Computational Science and Engineering*, Vancouver, BC, pp. 809-816, 2009.

[20] L. Buttya´n and I. Vajda, "Towards Provable Security for Ad Hoc Routing Protocols," in *Proceedings of the ACM Workshop Ad Hoc and Sensor Networks (SASN '04)*, 2004.

[21] G. Acs, L. Buttya´n, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," in *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, pp. 1533-1546, 2006.

[22] G. Acs, L. Buttya´n, and I. Vajda, "Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks," *European Workshop of Security and Privacy in Ad Hoc and Sensor Networks (ESAS 2005)*, vol. 3813, pp. 113-127, 2005.

[23] G. Acs, L. Buttya´n, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, pp. 1533-1546, 2006.

[24] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks*,"* *Wireless Networks*, vol. 11, pp. 21-38, 2005.

[25] C.H. Lin, W.S. Lai, Y.L. Huang, and M.C. Chou, "Secure Routing Protocol with Malicious Nodes Detection for Ad hoc Networks," *22nd International Conference on Advanced Information Networking and Applications-Workshops (aina workshops 2008)*, Okinawa, pp. 1272-1277, 2008.

BIOGRAPHIES OF AUTHORS

Kumaran U. He received the B.E. degree in Information Technology from the University of Anna university, Chennai 2009, and the M.Tech. degree in Computer Science and Engineering from the University of Anna university, Chennai, India, in 2014 and Ph.D. degrees in Computer Science and Engineering, Chennai, India, in 2018., He joined the Department of Computer Science and Engineering, as Assistant Professor in, Saveetha University, Chennai. Dr. U Kumaran is a Fellow of the International Association of Engineers, The Society of Digital Information and Wireless Communication and International Computer Science and Engineering Society. He was awarded as Young scientist by ICEACBS 2020 Organized by VOICE and PIAS.

Ramachandran A., working as an assistant professor in the department of computer science and engineering at B.S. Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Chennai, India.

J. Jegan received the B.Tech degree in 2006 from Anna University and M.E degree in 2009 from Anna University and Doctorate degree in computer science and engineering from Manonmaniam Sundaranar University, Tirunelveli, India, in 2018. He is a Associate professor in cse dept in sreenivasa institute of technology and management studies. He published more than 10 international journal papers. He is a member of ISTE chapter. He acts as a co-guide for research scholar. His current research interest in wireless sensor networks.

E. K. Subramanian received his B.Tech degree from Madras Institute of Technology, Anna University, Chennai in the year 1992 and M.E degree from College of Engineering, Anna University, Chennai in the year 2010. He is presently working at Saveetha School of Engineering, in the department of Computer Science as Assistant Professor (Senior Grade). He is currently pursuing his Ph.D at B S Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Chennai.