International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 6, Issue 3, March 2017 **ISSN 2319 - 4847**

A Novel Attack Independent Mobile Adhoc Network against Collaborative Black hole & Gray Hole Attack using Distributed Attack Resilient Routing Protocol

Ms N Rajeswari[1], Dr G Kalpana[2]

[1] Assistant Professor(Senior Grade),Department of Computer Applications,
PSG College of Technology,Coimbatore

[2]Associate Professor,Department of Computer Science,
Sri Ramakrishna College of Arts and Science for Women,Coimbatore

Abstract

Development of a secure routing protocol against collaborative Black hole attack and gray hole attack is considered as a more significant part of the Mobile Adhoc Network evolution to support next generation communication demand for packet transmission. The Malicious nodes detection has great challenges to detect the vulnerabilities and inabilities of the nodes. Therefore it is essential to model an effective security routing protocol to detect and prevent the nodes from anonymous behaviours in terms of proactive and reactive manner using a novel technique named as "Distributed Attack Resilient Routing protocol. The Distributed Attack Resilient Routing(DARR) protocol analyses and formulates the anonymous behaviours node by exploiting the knowledge from the routing table. The Routing table usually contains the path information and packet header information in the form of trace file. The packet loss degrades the network performance. Furthermore to ensure the data integrity, multiparty encryption algorithm provides a prominent solution to avoid the packet from losses and packet modifications. The primary goal of our approach is to reduce the detection time and improve the packet delivery ratio by eliminating the packet loss and jamming attacks. Distributed Attack Resilient Routing(DARR) model is data preserving and incurs low communication and storage overheads through utilization of data compression algorithm in the encryption model to secure the packet header and payload. The model achieves lower computational complexity. The simulations results proves that the Distributed Attack Resilient Routing(DARR) model outperforms the state of art approaches against the performance metrics such as No .of packet loss, Detection time and Detection accuracy.

Keywords: Mobile Adhoc Network, Attack Silent Network, Gray Hole Attack, Symbol Attack, Routing.

1. INTRODUCTION

In mobile ad hoc networks (MANETs), collaboration between nodes is the most important factor while sending packets among nodes. Mobile nodes communicate with each other using a multi-hop fashion [1]. Each node can forward data packets for other nodes. Mostly Nodes refuse communicate in the network for data communication by exhibiting the selfish behaviour and some case, the intermediate nodes may drop a packet or inject false data in order to generate a jamming to the network [2]. It is been utilized to analyse and develop a security protocol for data transmission against the malicious node in the network. This kind of attack is considered as motivation of the work in this research. Existing system even fail to produce efficient measurement due interference[3], collision[4] and node outage[5] when less no of node is allowed to sense and further it leads to biased conclusion. The cause of the existing system leads to model the proactive and reactive defense architecture using trace file. The Distributed Attack Resilient Routing(DARR) system is named as Distributed Attack Resilient Routing protocol which modelled to resolve the issues of the packet dropping attack at different strategies on the network by malicious node and with help of the multiparty data encryption algorithm the symbol attack can be eliminated as it works as intermediate node in order to generate the jamming on the network. The Collaborative attacks such as Black Hole attack [7] and Symbol attack [8] is eliminated using the proactive and reactive defense mechanism. The Distributed Attack Resilient Routing(DARR) approach mitigates the misbehaving node in the network in order to detect and prevent against attack propagation. The Distributed Attack Resilient Routing(DARR) Approach detects easily the malicious nodes which broadcasting the false injected information to the routing table. The routing table is used to analyse the path and predict the path for data transmission through route request packet and route replay packet. To execute the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the network. If an intermediate node has routing information to the destination in its route cache, it will reply with a RREP to the source node. When destination receives the RREQ, it can know each intermediary node's address among the route. The destination node relies on the collected routing information among the

packets in order to send a reply RREP message to the source node along with the whole routing information of the established route. The attack detected in periodically updated in the routing table for route maintenance. Any detected malicious node is kept in a black hole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. The Multiparty encryption algorithm encrypts the packet header information and payload of the data using different cryptography mechanism [9] in order to prevent the data from denial of service attack and packet inception. The rest of paper is organized as follows; section 2 explains the background knowledge regarding the related work. Section 3 explains and formulates the Distributed Attack Resilient Routing(DARR) System. The simulation results are discussed in section 4. Conclusion of the work along with future work of the paper was given in section 5.

.

2. RELATED WORKS

2.1Pro-active Approaches

The approach is based on the mechanism "Detect and Prevent ". It works as constantly monitors the traffic and detects the illegal activities through nearby or neighbor nodes. However, one of the advantages of these types of schemes is that it can help in preventing or avoiding an attack in its initial stage.

2.2Cooperative Bait Detection

Cooperative Bait Detection Scheme (CBDS), which aims at detecting and preventing malicious nodes launching gray hole/collaborative black hole attacks in MANETs. In this approach, the source node selects an intermediate node with data transmission has to be initiated, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message [10]. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique [11]. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again. The CBDS scheme merges the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps in order to reduce the resource wastage. CBDS is DSR-based routing protocol. As it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message. However, the source node may not necessary be able to identify which of the intermediate nodes has the routing information to the destination or which has the reply RREP message or the malicious node reply forged RREP.

3. PROPOSED MODEL- DISTRIBUTED ATTACK RESILENT NETWORK

3.1. Network Model

Mobile Ad hoc Networks is modeled with several nodes which is capable transmitting, receiving among nodes used as intermediate nodes. Each node in a MANET is free to move independently in any direction, and will therefore change its links to other nodes frequently. Each node must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each node to continuously maintain the information required to properly route traffic. Because of the infrastructure-less architecture of MANET, our risk-aware response system is distributed, which means each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET may isolate the malicious node, but others may still keep in cooperation with due to high dependency relationships. Nodes communicate both in unicast mode[12] and broadcast mode[13].

3.2. Black Hole Attack Strategies

It is a kind of the denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. Co operative Black hole means the malicious nodes act in a group [14]. It works by sending fake RREP with higher sequence number to the source node in order to pretend like a destination node, so, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself, due to this actual source and destination nodes are unable to communicate.

3.2.1. Gray Hole Attack

A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are:-

- ❖Dropping all UDP packets while forwarding TCP packets and another may be Dropping 50% of the distribution. These are the attacks that seek to disrupt the network without being detected by the security measures.
- ❖Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So can't able to identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node[15].

3.3. Symbol Attack Strategies

The adversary model can classify packets, before the packet transmission is completed. Once a packet is classified, the adversary may choose to jam it depending on his strategy. It is also a type of DDOS attack. There are many different attack strategies that a jammer can perform in order to interfere with other wireless communications [16]. Some possible strategies are exposed below:

- ❖Constant Jammer: A constant jammer continuously emits a radio signal that represents random bits; the signal generator does not follow any MAC protocol.
- ❖Deceptive Jammer: Different from the continuous jammers, deceptive jammers do not transmit random bits instead they transmit semi-valid packets. This means that the packet header is valid but the payload is useless.
- ❖Random Jammer: Alternates between sleeping and jamming the channel. In the first mode the jammer jams for a random period of time (it can behave either like a constant jammer or a deceptive jammer), and in the second mode (the sleeping mode) the jammer turns its transmitters off for another random period of time.
- ❖Reactive Jammer: A reactive jammer tries not to waste resources by only jamming when it senses that somebody is transmitting.

3.4. Distributed Attack Resilient Routing(DARR) Approach

Distributed attack resilient routing protocol which acts and prevention and detection framework against the collaborative black hole, gray hole and symbol attacks in the network. The Distributed Attack Resilient Routing(DARR) model uses the different node characteristic to initiate the transmission by sending multiple Route request packet and listening to multiple route replay packet [17]. Based on the analysis of replay packet, source node decides the data communication of the neighbour node based on

If (Node Capacity of N_i from N_{i-1}= = Node Capacity of N_{i+1})
Add N_i into Trust Node list
Else
Add N_i into malicious node list also eliminate it from the further data transmission

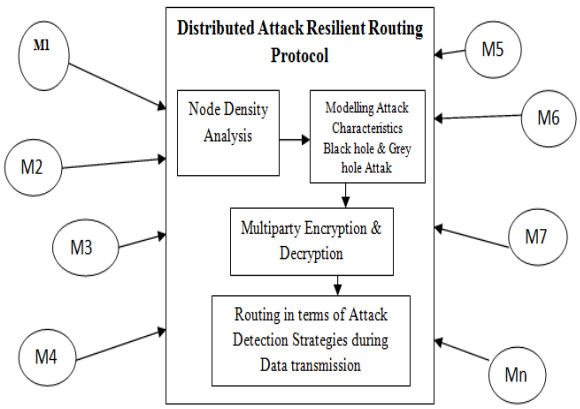


Figure 1 – Secure Routing Architecture of the Distributed Attack Resilient Routing Protocol

The reverse tracing mechanism helps in determining the black listed nodes. The trusted node is treated as reserved node. The node detection is carried out in the distributed region either splitting it into different zones or using entire region for data analysis. The differential operation is carried out on the nodes. The source node would then store the node in a black hole list and broadcast the alarm packets through the network to inform all other nodes to terminate their operation with this node.

3.4.1. Multiparty Encryption and Decryption

The multiparty encryption algorithm is performed on the both packet header and packet payload. It is carried out in order to save the data from packet loss and jamming attack injected by attacker to spoil the network traffic [18]. The Multiparty

encryption is carried out the data transformation using asymmetric cryptography technique; the representation of the encryption working model is depicted below

1. Consider M as packet with payload and packet header
2. Compute for payload and Packet header size

$M^{|}$ is updated from each intermediate node periodically using f(x) w.r.t to Time is denoted as p^{o}
X denotes the time
3. Calcualte P^{o} =f(x)
4. Cipher text for multiparty encryption is given by €

∂ --→Original payload or packet header
€ =∂ +£
Where £ is encryption logic based attributes of data
£= $\sum \alpha$

Packet Header Encryption
The packer header encryption is carried out in the sender side in order to secure the information from DDOS attacks in the network , working module of encryption is given below

1. Get the text value of the Data to be encrypted and randomly add 1 or 2 to each data at sender side.
2. Record the number of packet chunks present in the packet. Group the text and convert to single large integer value for each group.
3. Convert text to be group using Mathematica is given by gr p = Length [IntegerDigits[p, 258]] − 1
Pair up the result obtained from step 2 and store as 'Pm' which is the plain message input
4. Select a random 'k' and compute 'kG' and 'kPb' where 'Pb' is the public key of the receiver.
5. Perform point addition of 'kPb' with each value of 'Pm' and store as 'Pc' which is the cipher text.
6. Convert the cipher text list from step 5 to value.
7. Pad left with 0 to each list from step 6 which have less than gr p + 1 number of elements, to make each list equal in length.
8. Flatten the list from step 7, group them according to the number of text chunks that have recorded and partition them to width of the plain text.
9. Convert the values from step 8 into cipher text.

Packet Header Decryption
The Cipher text is decrypted using the mapping table in the received side. Mapping table generates the text value from the cipher text

1. Get the text value of the cipher Text and group by gr p + 1 number of Chunks and form single big integer value for each group. Record the number of chunks of the cipher text.
2. Pair up the value obtained from step 1.
3. Perform point multiplication of 'kG' with 'nB' where 'nB' is the private key of the receiver.
4. Perform point subtraction between values from step 2 with value from step 3.
5. Get the value from step 4 with base 258 and subtract random 2 from each value.
6. Group the flatten value obtained in step 5 in term of recorded number of chunks of the cipher text and partition them to the width of the cipher text.

4. SIMULATION RESULTS

The Distributed Attack Resilient Routing(DARR) model is simulated on the NS2 simulator to study & analyse the effectiveness of the malicious node detection and prevention in terms of their performance in a variety of network parameters of the mobile AdHoc Network [19]. In this simulation 40% of nodes is considered as malicious nodes. Nodes are distributed uniformly at random in a square of area 5* 5 with node density n_d=3. Also attacks have been placed in the network with density n_e. The Distributed Attack Resilient Routing(DARR) Environment is detailed in the Table 1

Table 4.1: Simulation Parameters used to build a protocol

Simulation Parameter	**Value**
Simulator	NS2
Topology Size	1000m *1000m

Number of Nodes	150
Bandwidth of the Network	2Mbps
Traffic type	CBR
Pause Time	0s
Packet size	512 bytes

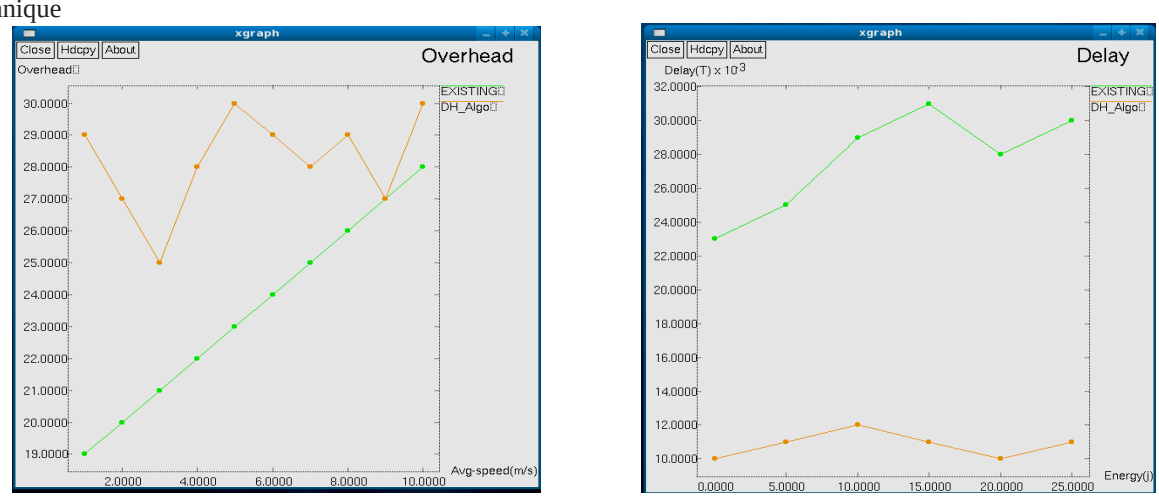
The performance of secure routing protocol against various security and routing metrics are discussed below

Routing Overhead and Delay

Routing overhead refers to performance metric to the percentage difference between total energy used by different protocols with respect to the benchmark. The delay of Distributed Attack Resilient Routing(DARR) attack detection mechanism against attack estimation in the packet transmission leads to delay in the network. The figure 2 describes the performance analysis of the network operation against the delay and network overhead.
The routing over head is calculated as follows

$$\text{Routing overhead } R_d = 100\% * \frac{nd - ne}{nd}$$

Where nd is the energy of the Distributed Attack Resilient Routing(DARR) technique & ne is the energy of the existing technique

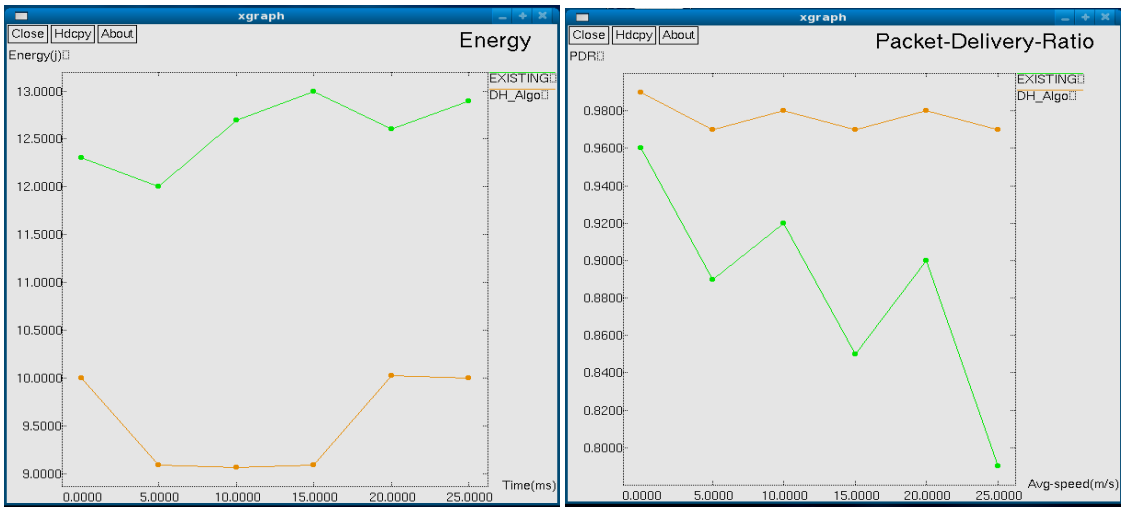


(a) **(b)**

Figure 2. Simulation Outcome of the routing overhead in fig 2a and Delay in fib 2b against the Cooperative Bait Detection Scheme and Distributed Attack Resilient Routing Approach

Energy Utilization and packet Delivery Ratio

Prediction of energy consumption of Distributed Attack Resilient routing protocols is carried out through the energy balanced factor is determined in terms of the residual energy of nodes and based on sensing cycle of the nodes in handling the transmission and attack detection [20].



(a) **(b)**

Figure 3: Simulation Outcome of the Energy in fig 3(a) and packet Deliver ratio in fig 3(b) against the Cooperative Bait Detection Scheme and Distributed Attack Resilient Routing Approach

The measurement proves system which balances the energy consumption, prolongs the function lifetime and guarantees high QoS (such as Energy-Balanced, Long-Surviving and Packets Reception Radio) of MANET. The energy utilization is described in the figure 3. The Packet Delivery ratio represents the ideal case where the attackers are identified and completely isolated in the network to explain the efficiency of the Distributed Attack Resilient Routing(DARR) routing mechanism and serves as the baseline for evaluating the impact of the attack and the performance of Distributed Attack Resilient Routing(DARR) defense scheme such as

- ❖Packet Drop: The attackers drop data packets, but participate in the protocol as benign nodes. The attack has effect only when attackers are selected based on the principle. The scenario demonstrates that metric manipulation amplifies data dropping attacks as described in the figure 3
- ❖ **Packet Delivery ratio** = Sum of time taken by each node in the path during transmission / No .of packets for transmission

The packet delivery ratio is computed for Distributed Attack Resilient Routing(DARR) system using the attack elimination mechanism. The attack nodes are collected in the different cluster for data transmission with high transmission rate and high node density is selected to increase packet delivery rate.

Throughput

Throughput of routing algorithm is to find the shortest path in terms of the less transmission rate by ignoring the attacks in the network, where attacks eliminated with basis of probability measures to allocate it into the attack list. The Throughput also depends upon the end to end communication.

In the experiments, the system evaluates the effect of malicious nodes against the data transfer.

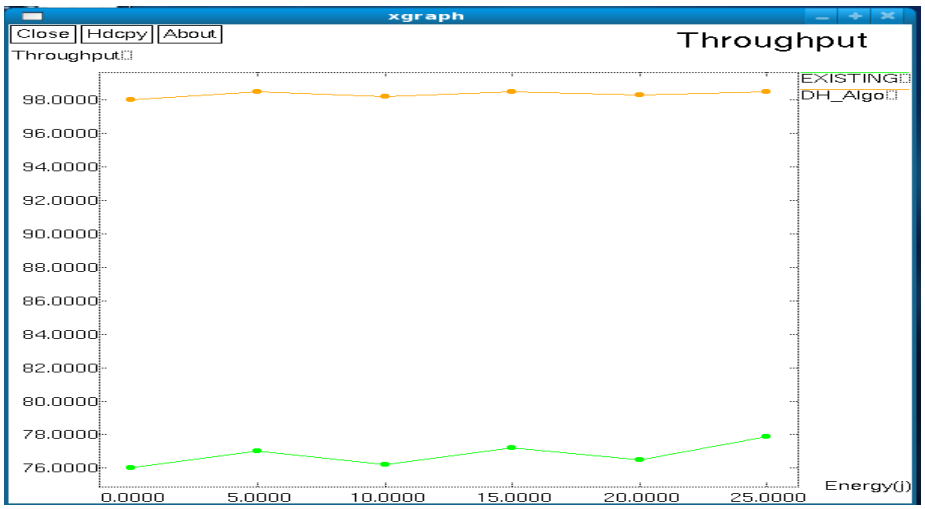


Figure 4. Simulation outcome of the Throughput of the Cooperative Bait Detection Scheme and Distributed Attack Resilient Routing Approach

The fig 4 provides the performance of the security methods.

Throughput = Bandwidth of the receipt Node * Round trip Time of path

The Communication efficiency of the routing protocol is measured in terms of throughput of the

Mobile Adhoc Network against the malicious attack

Table 4.2. Performance analysis of the energy Balancing Technique

Technique	Packet Delivery ratio	Energy	Routing Overhead	Throughput
Distributed Attack Resilient Routing Approach -Proposed	**23ms**	**12bps**	**12ms**	**45mbps**
Cooperative Bait Detection Scheme – Existing	**28ms**	**14 bps**	**14ms**	**37mbps**

.

The Throughput obtained in the system is calculated based path selection and data transmission. The performance values of the metric computed against various techniques is depicted in the table 4.2 which gives clear vision of the improvement in the energy management and network lifetime extension. It is dynamic to changes such new sensing node added in the network.

5.CONCLUSION

The authors had designed and simulated the Distributed attack resilient routing protocol to prevent and detect the malicious attacks propagating in the network such as collaborative black hole and symbol attacks. This work gives solutions to ensure the data integrity and data confidentiality during data transmission by enabling the asymmetric encryption named as multiparty encryption algorithm to avoid the packet fom losses and packet modifications which carried out using addition or injection of data into packet or group of packets. Distributed Attack Resilient Routing(DARR) model preserves the data and incurs the low communication and storage overheads through utilization of data compression algorithm in the encryption model in order secure the packet header and payload. The simulation results has proved that Distributed Attack Resilient Routing(DARR) model outperforms the state of art approaches against the performance metrics such as No .of packet loss, detection Time and detection accuracy. Future work may extend this model from several aspects such as resisting multiple attacks, which will be helpful to design secure protocol.

References

[1] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013).
[2] X. Wu and D. K. Y. Yau, Mitigating denial-of-service attacks in MANET by incentive-based packet filtering: A game-theoretic approach, In Proc. 3rd International Conference on Security and Privacy in Communications Networks, Nice, France, September 2007.
[3] K. Lee, J. Kim, K.H. Kwon, Y. Han, and S. Kim, "DDoS Attack Detection Method Using Cluster Analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.
[4] K. Lee, J. Kim, K.H. Kwon, Y. Han, and S. Kim, "DDoS Attack Detection Method Using Cluster Analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.
[5] C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649-1662, Dec. 2007.
[6] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," IEEE/ACM Trans. Networking, vol. 19, no. 2, pp. 512-525, Apr. 2011.
[7] S.T. Sarasamma, Q.A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," IEEE Trans. Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 35, no. 2, pp. 302-312, Apr. 2005.

[8] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073-1080, June 2012.
[9] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.
[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.
[11] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.
[12] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.
[13] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.
[14] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.
[15] H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007, pp. 362–367.
[16] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Pers.Commun., vol. 29, pp. 367–388, 2004.
[17] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. WiSec, 2009, pp. 103–110.
[18] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.
[19] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.
[20] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Routing amid colluding attackers," in Proc. IEEE Int. Conf. Network. Protocols, 2007, pp. 184–193.

AUTHOR

N Rajeswari had received the B.Sc and M.Sc Applied Sciences and Computer Technology Degrees from Bharathiar University and Anna University in 2002 and 2004 respectively.During 2004-2005 worked as lecturer in Department of Computer Science,Sri Krishna College of Arts and Science.From 2005 till date was working as Assistant Professsor in the Department of Computer Applications,PSG College of Technology.Has guided many projects at UG and PG Level.Her research interest includes Computer Networks,Mobile Networks.

Dr.G.Kalpana is the Associate professor in the Department of Computer Science, Sri Ramakrishna College of Arts and Science for women, Bharathiar University, India. She obtained her Ph.D degree in computer science in the year 2014 from Anna University. She has published papers in various journals (indexed by Thomson Reuters and Scopus) and conference proceedings (Springer Digital Library). Her research interests are in the area of Networking and Data mining.