Trust based Routing in Wireless Ad Hoc Networks under Adverse Environment

D. Sylvia
Research Scholar
Jawaharlal Nehru
Technological University
Hyderabad

Jeevaa Katiravan
Associate Professor
Department of Information
Technology
Velammal Engineering College
Chennai

D. Srinivasa Rao
Department of Electronics and
Communication Engineering
Jawaharlal Nehru
Technological University
Hyderabad

ABSTRACT
In wireless ad hoc networks, traditional routing considers hop count and distance for making the route selection. The network is prone to various types of attacks by intruders in which packets maybe modified or dropped. A trust based mechanism maybe employed in which the nodes are constantly monitored for malicious behaviour. An abnormality in the behaviour of the intermediate node effects the trust value and such malicious nodes that are detected maybe excluded from the route and a new route discovery maybe initiated. In this paper, such a trust based routing is proposed to detect network layer attacks. A route discovery is initiated under the detection of malicious nodes as against the use of control packets for route rediscovery. Using simulation, it is proved that the proposed scheme achieves better performance in terms of Packet Delivery Fraction, end-to-end delay and therefore improves the performance of the network under adverse environment

Keywords
Wireless Ad Hoc Network, Trust Calculation, Attacks, Detection

1. INTRODUCTION
Wireless communication has been witnessing a dramatic increase in usage, especially because of the increasing number of mobile users who demand ubiquitous access to services. This deployment includes disaster relief operations ,military operations, emergency search and rescue missions ,interactive conferences and conventions, etc.[1] Wireless ad hoc network is type of a network characterized by a decentralized, infrastructure independent and self-configuring network. The nodes cooperate among themselves in forwarding the packets, due to the lack of a centralized control. Ad hoc networks are constrained by the scarce availability of resources such as bandwidth and power. The channel, being shared by all the nodes in the transmission region, places limits on the available bandwidth, as it depends on the number of transmitting nodes and the amount of traffic handled by the network. The lack of centralized control in the wireless channel also makes the wireless network more prone to attacks than the wired network. Security issues become important in such networks. The routing protocol must provide the required amount of Quality of Service in terms of bandwidth, packet delivery ratio, throughput and energy of the network, while also considering the possibility of attacks. Security takes up the utmost importance in an ad hoc network, since it is more vulnerable to attacks than the wired networks. A wired network has defences in terms of firewalls and gateways, whereas a wireless link is more vulnerable to various range of attacks. An ad hoc network is termed to be secure when it is able to take care of different security issues such as confidentiality of the nodes in communication, integrity of data, availability of resources and authentication of the communication devices.
The advancements in technology not only provide new capabilities to the users but also provide an opportunity to malicious intruders to attack critical information resources. The dynamic nature of the wireless ad hoc network gives space for research on the attack strategy and its effect on the network performance.

Routing in ad hoc network has been actively researched and yet the deployment of such networks faces major issues which include, limited resources in terms of power, bandwidth and usage, mobility of the nodes and limited security. The performance of a ad hoc network is affected by the medium access scheme, routing, quality of service, security, energy management, scalability and deployment consideration.[1]

The major objective of our work is to introduce an attack model in wireless ad hoc network and the focus is on the development of a routing protocol which considers traffic capacity improvement, provides quality of service and security measures against network layer attacks.

2. MATERIALS AND METHODS
The Ad Hoc networks lack a centralised infrastructure. All nodes cooperate among themselves to forward the packets within the transmission range. The mobility of the nodes which causes frequent path failures and construction of new routes, makes the design of the routing protocol very important for the efficient transmission of the packets within the network. The major issues in designing a routing protocol include mobility of the nodes, resource constrains in terms of bandwidth and power and error in the broadcast channel.[2] The nodes must be capable of providing a bandwidth, power aware secure routing for achieving the maximum capacity of the network.
Various routing protocols have been proposed in the literature [3] and this section describes the secured version of the dominant routing protocols available for the wireless ad hoc networks. Table 1 summarizes the secure routing protocols considered.

Table 1. Popular secure routing protocols

Secure Routing Protocol	Type of Ad Hoc Routing	Base Protocol
QoS Route Discovery	Reactive	DSR
SQoS Route Discovery	Reactive	DSR
Ariadne	Reactive	DSR
Confidant	Reactive	DSR
CORE	Reactive	AODV
SAODV	Reactive	AODV
SAR	Reactive	AODV
PRAODV	Reactive	AODV
SEAD	Proactive	DSDV
SLSP	Proactive	OLSR
SRP	Hybrid	ZRP

2.1 Reactive Routing Protocol

One of the major on demand routing protocol is Dynamic Source Routing [4], which eliminated the periodic table update messages and thereby conserved the bandwidth consumption by control packets. Some of the secure protocols based on DSR are QoS Guided Route Discovery [5],Securing Quality of Service Route Discovery [6], Ariadne [7] and CONFIDANT [8].In Qos-guided route discovery protocol, a node is allowed to specify the desired QoS metrics, which must be provided by the selected path. It uses bandwidth, latency and jitter as the metrics but had difficulty in determining the resources available at a particular node. Securing Quality of Service Route Discovery [23] is a secure form of on demand routing protocol, which implements symmetric cryptography. It includes bandwidth and latency in the route computation process, but has not given due consideration to the capability of intermediate node in terms of node power, memory and storage. Ariadne [27] is a secure on demand protocol, based on the efficient broadcasting scheme TESLA. Ariadne has no feedback mechanism and has no knowledge of attacks on the discovered route. CONFIDANT (Cooperation of nodes fairness in dynamic adhoc network): categories nodes into selfish and unselfish nodes and uses global reputation values. It takes care of optimal forwarding and traffic diversion, by identification of routing misbehaviour.

AODV [9] is a dominant on-demand routing protocol that uses a destination Sequence Number to establish paths to the destination node. The utilization of resources is not optimal and also there is no provision of security in AODV. CORE[10] ,SAODV[11] ,SAR[12] PRAODV[13] are the secure versions of the AODV routing protocol.

CORE [10] implements a mechanism based on reputation, which ensures cooperative communication of nodes, thereby eliminating selfish behaviour. The watchdog mechanism it employs detects misbehaving nodes at both forwarding and link level, but does not perform well in the presence ambiguous collisions and limited transmission power. SAODV[10] dealt with black hole attack, in which the intermediate cannot send a RouteReply message. The protocol was optimal for black hole attack but failed in the presence of wormhole attack.

Security Aware Ad-Hoc Routing (SAR) protocol [12] selects routes on the basis of trust levels, which are security attributes assigned to nodes. It can be implemented in any routing protocol but the encryption techniques employed give rise to increased overhead at any node. PRAODV[13], an enhanced version of AODV provides improved performance by reducing the path breakages by the prediction of link lifetime using velocity and location information as additional parameters.

2.2 2.2 Proactive Routing Protocol

DSDV[14] and OLSR[15] are the prominent proactive or table driven protocols, in which routing tables are maintained by every node, which contains routing information and is periodically updated.

SEAD (Secure Efficient Adhoc Distance Vector Routing Protocol) [16],based on DSDV, focuses on DoS and resource consumption attacks. It uses a one way hash function and avoids routing loops, but is not optimal when the attacker uses the most recent update metric.

SLSP [17] is a secure protocol, based on OLSR and it uses digital signature and one-way hash chains to ensure the security of link-state updates. This protocol improves the integrity level of MAC but the nodes that generate lesser link updates are given priority over the nodes that generate more link updates.

2.3 Hybrid Routing Protocols

The best features of reactive and proactive routing protocols are considered in the Hybrid routing protocols such as ZRP[18]. These protocols maintain local information within the routing zone, while establishing paths on demand outside the routing zone.ZRP provides improved detection and prevention of overlapping queries and less delay, but does not consider security. SRP [19], the secure version of ZRP attempts to utilise a route maintenance function to maintain the secure route.

2.4 Security Issues in Wireless Ad Hoc Networks

The attacks in wireless networks are generally classified into active and passive attacks.

Passive attacks are just observation of the activities of the network and maybe difficult to detect, unless the malicious node interferes with the operation of the network. Active attacks, which aim to disturb the operation of the network, are more harmful in nature. The various attacks maybe classified [1] as listed in Table.2

Table 2. Classification of Attacks

SECURITY ATTACKS	
Passive Attacks	**Active Attacks**
Snooping	• Jamming • Wormhole Attack • Black hole Attack • Byzantine Attack • Information disclosure • Resource consumption attacks • Routing attacks • Session hijacking • Repudiation • Denial of Service • Impersonation • Device tampering • Manipulation of network traffic

Jamming is a MAC layer attack, in which a malicious node transmits signals at the same frequency as the sending node, thereby causing errors in the desired transmission.

Wormhole is a network layer attack in which the packets are retransmitted between two colluding attackers, which causes failure in finding valid routes. Another network layer attack is black hole, in which an adversary propagates false routes, disrupting the path finding process. Byzantine attack also targets the network layer causing loops and non-optimal paths. The resource consumption attack is highly detrimental to the network in terms of its resources. It targets the limited resources of the wireless networks such as bandwidth and power, by means of unnecessary route requests, relaying of stale packets and keeping the nodes always busy, depriving the nodes of its energy. The routing attacks maybe in terms of routing table overflow, routing table poisoning, packet replication, route cache poisoning and rushing attack.

In the transport layer, the intruder takes over the session between two nodes by impersonating on one end of the communication. Repudiation is the denial of the node in communication. Yet another serious attack is the epidemic attack[20] in which the malicious nodes inject polluted packets and therefore drain the network of its available resources.

Apart from these attacks briefly overviewed, several multilayer attacks also exist. Denial of Service attack [20, 21]is the most prominent of these, in which the authorized nodes are denied service by flooding of packets, jamming of signals, route disruption, etc. This attack results in the reduction and starvation of authorized use of the network resources. This attack can be categorized into three main types[22] as those that target the battery power of the network, by continuously sending pseudo packets to a node with the sole intention of depleting the energy resource of the communicating node, those that target Storage and Processing resources and those that Targets the bandwidth of the network and disturbs the connectivity of the network. The Distributed Denial of Service Attack [23] is an attack that tries to degrade the network resources by sending packets from several sources. Such an attack is to be given great consideration, especially because the wireless networks is resource constrained in terms of bandwidth and power.

Considering the compelling need of addressing the network layer security issues in MANET, this paper proposes a novel trust based mechanism called Trust Based AODV [TAODV] that implements cooperative communication between nodes and detects the network layer attack and C worm attack [24] and thereby improves the network performance.

2.5 Proposed Methodology

Traditional routing protocols discovers routes based on hop count, with no due consideration for the quality of the path selected. QoS aware routing , which considers trust value of the nodes can be very beneficial. The proposed methodology chooses the relay node based on a trust metric and a trust value is assigned for the authorized nodes. The algorithm consists of selection of forwarding relay nodes, calculation of trust value and detection of malicious attack. The flow diagram of the proposed methodology is shown in Figure 1.

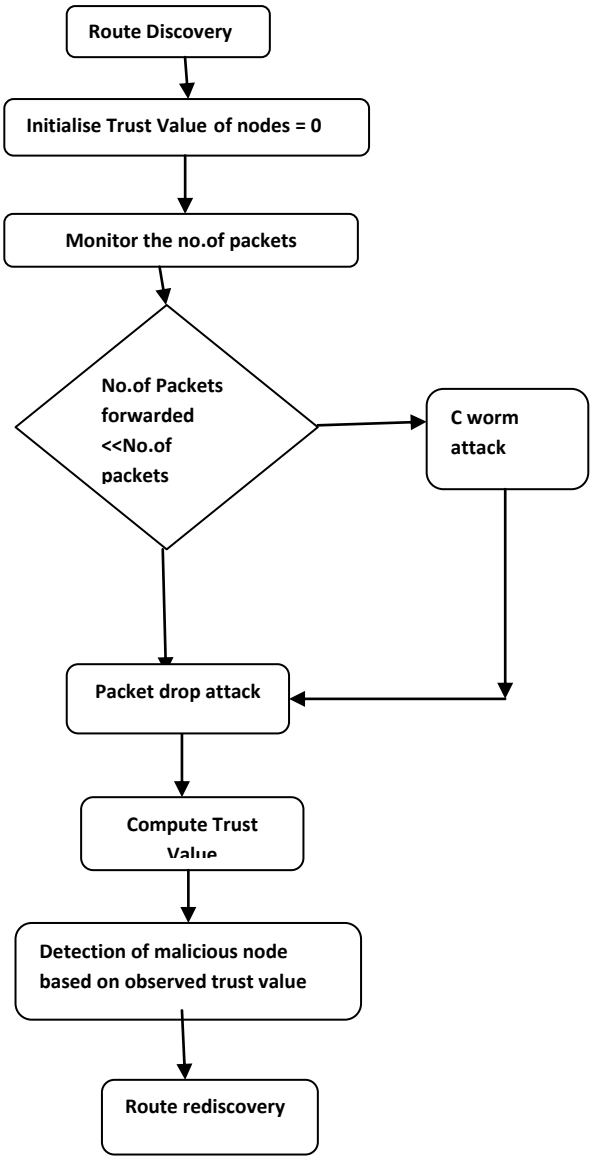

Fig 1: Flow Diagram of Proposed Methodology

Once a route has been established between the source and destination using the route request and route reply packets the data packets are forwarded along the optimal path choosen in which each node knows the next hop to which the packet is to

be forwarded. To maintain the QoS of the network , it becomes essential that the relay nodes forward the packets correctly. One of the active attacks, called packet dropping attack proves to be very costly to the network as the malicious attacker node drops the packets instead of forwarding them. This has a very detrimental effect. The C worm is a type of attack in which the number of packets transmitted is twice the normal traffic. In our proposed scheme every node maintains a Trust Table based on Trust metric which is simply the ratio between the number of packets successfully transmitted by the node to the total number of packets received for forwarding by the node.

The nodes in the network monitor the behaviour of its neighbouring nodes. When the malicious node which is in the forwarding path starts dropping packets, its trust value decreases. When the packet transmission is abnormal it indicates that the node could be suspicious, but immediately cannot be determined as malicious node since the abnormality could be due to several reasons such as intentional packet drop by malicious attacker, due to buffer overflow, congestion, channel conditions or simply timeout of the sending node.

Let n_r be the number of packets received at a node, n_f be the number of packets forwarded at a node, n_d be the number of packets dropped at a node.

A node monitors the number of packets received and forwarded by its neighboring nodes. Then the number of packets dropped is given by

$$n_d = n_r - n_f \quad (1)$$

The trust value is computed as follows:

$$Trust\ Metric = \frac{n_f}{n_r} \quad (2)$$

$$Trust\ Value = \begin{cases} 1, if\ Trust\ Metric \geq Threshold \\ 0.5, if\ Trust\ Metric = Threshold \\ 0, if\ Trust\ Metric \leq Threshold \end{cases} \quad (3)$$

When the trust value drops, the node is considered to be malicious and can no longer act as relay node. Therefore a route rediscovery is initiated immediately for selecting another legitimate node as relay node.

3. RESULTS AND DISCUSSION

The proposed scheme has been implemented by using Network Simulator ns-2.35. In the simulation setup, malicious node behaviour is implemented by packet drops at the network layer. The various parameters used in the simulation are shown in Table 3.

Table 3 : Simulation Parameters

Parameters	Value
Simulation duration	200 s
Topology	1000 x 1000 m
Number of mobile nodes	40
Transmission range	250M
Movement model	Random WayPoint
Traffic type	CBR
Data payload	512 bytes/packet
Number of malicious nodes	2 to 10
Maximum speed of a node	5 m/s to 50 m/s

3.1 Packet Delivery Fraction

The performance of the network is analysed with and without the presence of malicious nodes in a mobile environment where the node speed is varied between 5 to 50 m/s..We find that the Packet Delivery Fraction which is a measure of the packets delivered to the packets generated. As shown in figure 2 ,the PDF under packet drop attack is significantly low which shows the packets dropped due to malicious nodes and more no of packets are delivered under the C-worm attack.

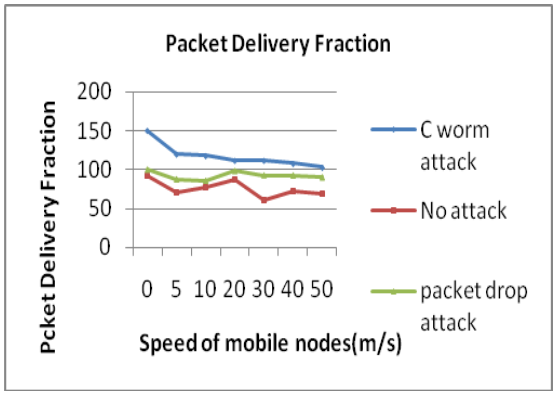

Fig 2 : PDF with and without attack

3.2 Average Throughput

The average throughput is the measure of the number of packets delivered successfully in the simulation time. We compare the throughput obtained under attack in which the no.of malicious node is varied from 2 to 10. As shown in figure 3,the throughput of the network decreases when the number of attackers increases.

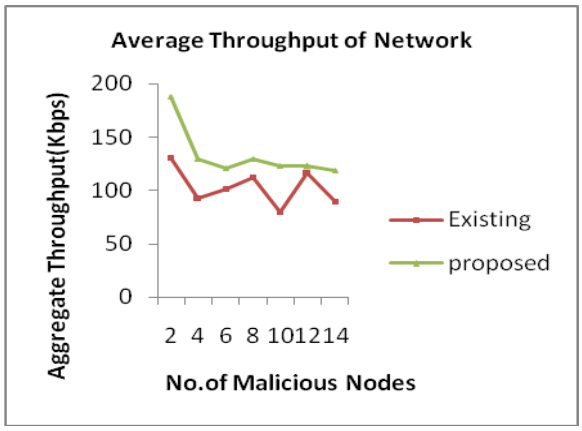

Fig 3 : Average Throughput Vs No.of Malicious Nodes

The end-to-end delay is the delay incurred for the transmission of the packets from source to destination. Due to the malicious node detection, ,the proposed TAODV achieves lesser delay of 3% when compared to the existing scheme due to the earlier route discovery initiated under the detection of attack as shown in figure 4.

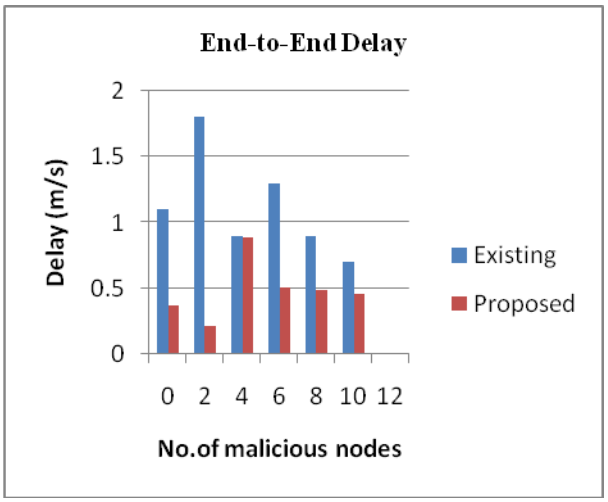

Fig 4 : End-to-End Delay Vs No.of Malicious Nodes

The Normalised Routing Overhead gives an evaluation of the extra overhead incurred due to the additional computation of the algorithm. As shown in Figure 5,the overhead is only 2% more than the existing protocol, which becomes insignificant when compared to the improvement achieved in PDF.

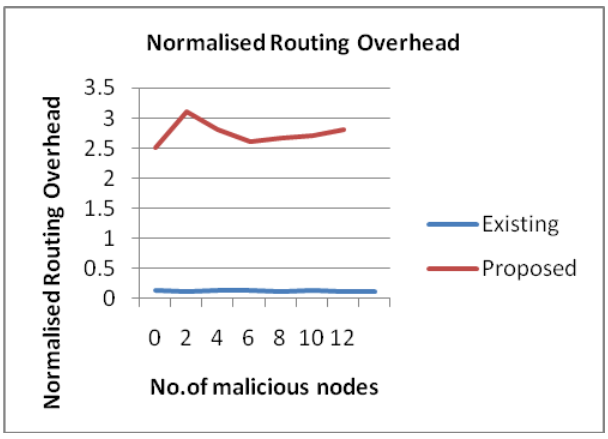

Fig 5 : Normalised Routing Overhead Vs No. of Malicious Nodes

From the various studies carried out, it is shown that the proposed scheme outperforms the existing scheme in improving the QoS of the network.

4. CONCLUSION

This paper proposed a Trust Based Routing Scheme called Trust Based AODV (TAODV), in which a trust metric is assigned to the nodes based on the behaviour of the nodes. An abnormal behaviour initiated a route rediscovery and therefore such an optimal scheme is found to have significant improvement in various QoS metrics when compared to the existing scheme. The performance of TAODV has been ,assuming there is no loss of packets dur to insufficient energy of the nodes. Future work would be to analyse the performance of the network when the nodes have insufficient energy to forward the packets.

5. REFERENCES

[1] S. Murthy, C. Siva Ram, and B.S.Manoj, “Ad Hoc Wireless Networks : Architectures and Protocols”, Prentice Hall, 2004.

[2] Y. Hu and A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing,”IEEE Computer Society, 2004.

[3] L. Abusalah, A. Khokhar and M. Guizani, “A survey of secure mobile ad hoc routing protocols,” IEEE Commun. Surveys and Tutorials, Vol.10, no. 4, pp. 78-93, 2008.

[4] D. B. Johnson and D. A. Maltz, “Dynamic Sources Routing in Ad Hoc Wireless Networks,” Mobile Computing, 1996.

[5] D. A. Maltz, “Resource Management in Multi-hop Ad Hoc Networks,”CMU School of Computer Science Technical Report CMU-CS-00-150,Nov. 21, 1999.

[6] Y. Hu and D. B. Johonson, “Securing Quality-of-Service Route Discovery in On-Demand Routing for Ad Hoc Networks,” Proc. ACM SASN‘04, Oct. 20, 2004.

[7] Y. Hu, A. Perrig, and D. B. Johonson, “Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks,” Proc. ACM MobiCom ‘02,Sept. 23–26, 2002.

[8] S. Buchegger and J. L. Boudec, “Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes-Fairness In Dynamic Ad-hoc Networks,” Proc. IEEE/ACM Symp. Mobile Ad Hoc Networking and Computing (MobiHOC), 2002.

[9] C. E. Perkins and E. M. Royer, “Ad-Hoc On-Demand Distance Vector Routing,” Proc. 2nd IEEE Wksp. Mobile Computer Systems and Applications,1999, pp. 90–100.

[10] P. Michiardi and R. Molva,, “CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks”, IFIP-Communication and Multimedia Security Conf. ,2002.

[11] M. Guerrero Zapata, “Secure Ad hoc On-Demand Distance Vector Routing,” Mobile Computing and Commun. Review, Vol. 6, No. 3.pp.106-107

[12] S. Yi, P. Naldurg, and R. Kravets, “A Security-Aware Routing Protocol for Wireless Ad Hoc Networks,” Proc. ACM MobiHoc ’01, 2001.

[13] Vinod Namboodiri, Manish Agarwal, Lixin Gao, “A Study on the Feasibility of Mobile Gateways for Vehicular Ad-hoc Networks”,VANET’04, October 1, 2004, Philadelphia,Pennsylvania,USA.

[14] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” ACM SIGCOMM ’94, 1994.

[15] T. H. Clausen et al., “The Optimized Link-State Routing Protocol, Evaluation through Experiments and Simulation,” Proc. IEEE Symp. Wireless Personal Mobile Communications 2001, Sept. 2001.

[16] Y. Hu, D. B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” Proc. IEEE Mobile Computing Systems and Applications, 2002, pp. 3–13.

[17] P. Papadimitratos and Z. J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," Proc. IEEE Wksp. Security and Assurance in Ad Hoc Networks, in Conjunction with the 2003 Int'l. Symp. Applications and the Internet, Jan. 28, 2003.

[18] Z. J. Haas and M. R. Pearlman, "The zone routing protocol: A hybrid framework for routing in ad hoc networks," in Ad Hoc Networks, C. E. Perkins, Ed. Reading, MA: Addison-Wesley, 2000.

[19] Y. Hu and D. B. Johonson, "Securing Quality-of-Service Route Discovery in On-Demand Routing for Ad Hoc Networks," Proc. ACM SASN '04, Oct. 20, 2004.

[20] Yongkun Li; Lui, J.C.S., "Epidemic Attacks in Network-Coding-Enabled Wireless Mesh Networks: Detection, Identification, and Evaluation," IEEE Transactions on Mobile Computing, vol.12, no.11, pp.2219,2232, Nov. 2013.

[21] M.K. Denko, "A Localized Architecture forDetecting Denial of Service (DoS) Attacks in WirelessAd Hoc Networks", In Proc. IFIP INTELLCOMM'05,Montreal,Canada,2005.

[22] Carl G., Kesidis G., Brooks R., and Rai S., "Denialof Service Attack Detection Techniques," ComputerJournal of IEEE Internet Computing, vol. 10, no. 1, pp.82-89, 06.

[23] Khan, Rizwan, and A. K. Vatsa. "Detection and control of DDOS attacks over reputation and score based MANET." Journal of Emerging Trends in Computing and Information Sciences 2.11 (2011): p9-12.

[24] Kaur, Gurjinder, Yogesh Chaba, and V. K. Jain. "Distributed Denial of Service Attacks in Mobile Adhoc Networks." World Academy of Science, Engineering and Technology 73 (2011): 725-727.

[25] Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan, and Wei Zhao "Modeling and detection of camouflaging worm", IEEE transactions on dependable and secure computing, vol. 8, no. 3,Mmay/June 2011.