IJCSI International Journal of Computer Science Issues, Volume 13, Issue 3, May 2016
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org http://dx.doi.org/10.20943/01201603.3138

A Secure & Robust Scheme to Isolate DDoS Attacks Over MANET

Suveg Moudgil[1], Dr. Sanjeev Rana[2]

[1] Research Scholar, CSE Deptt. M. M. University. Mullana. Ambala, India – 133207

[2]Professor, CSE Deptt. M. M. University, Mullana, Ambala, India - 133207

Abstract

A Mobile ad-hoc Networks (MANETs) are self-configuring, infrastructure less networks consist of mobile nodes which communicate with one another through wireless medium. MANETs have several unique characteristics including dynamic topology, limited bandwidth and limited power of mobile nodes. Security is the biggest challenge in MANETs due to its features. The security of information of both the source and destination themselves, and the information handled by intermediate nodes, is becoming ever more important. Network security plays a crucial role in this. The traditional way of protecting the networks through firewalls and encryption software is not adequate. In this paper, we have studied the effect of different DDoS Attacks in the Ad hoc Networks. We have proposed solution that tries to eliminate the effect of these DDoS Attacks by monitoring and selection scheme using trust assignment scheme and robust random early detection scheme to isolate malicious node from the network over OLSR routing protocol. We have analysed the proposed scheme through simulation using ns2 simulator.

Keywords: DDoS Attack**,** MANET, OLSR, QoS

1. Introduction

Over the last two decades, mobile wireless communication has grown dramatically, from a small niche technology to a massive industry. Mobile devices are now ubiquitous, and the division between Personal Computers, PDAs, mobile cellphones and other mobile devices is not clear. Against this background, the security of information of both the devices themselves, and the information handled by these devices, is becoming ever more important. Security for mobility becomes the urgent requirement of this industry. Providing entity authentication and authenticated key exchange among nodes are both target objectives in securing ad hoc networks. It is difficult to use one encryption solution that always has the best performance in such a dynamic environment.

Wireless ad hoc networks have drawn a lot of attention from both research communities and the industry in recent years. They do not relying on any pre-existing communication and computing infrastructures. They allow autonomous peers to communicate with other peers over wireless links & to assist communications among others when required. MANETs are infrastructure less communication networks in which mobile nodes communicates with each other. MANETs are characterized by dynamic topology, limited bandwidth, limited battery power & computation resources of nodes & error prone transmission medium [1]. They uses multi-hop routing. Each Intermediate node acts as a router. All these factors make the routing in MANETs a challenging task. Most of routing protocols in MANET use shortest path or minimum hop routing. Major drawback of existing MANET shortest path routing protocols is that they consider the path with minimum no. of hops as optimal path to any given destination. The fewer innermost nodes becomes the backbone for most of the traffic, leading to congestion. This leads to higher end to end delays, lower packet delivery and higher routing overhead. The heavily loaded nodes have high power consumption which reduces battery power. It increases no. of dead nodes in the network which further creates network partitions. Load balancing is essential to avoid traffic congestion problem. With load balancing, traffic congestion and load imbalance can be minimized resulting in better network throughput, minimize end to end delays, mobile node life time can be maximized. Thus, increasing the overall network life time.

Wireless ad hoc networks, are prone to various passive and active attacks due to the shared wireless medium, absence of properly-protected media and well-trusted infrastructures. It can compromise the confidentiality, integrity and authenticity of information exchange among participating nodes. Also, in some wireless ad hoc networks, the nodes can become selfish, greedy and even tampered by adversaries, which brings more challenges to secure the wireless ad hoc network. Many efforts have been dedicated to secure peer communications in wireless ad hoc networks. These solutions belongs to symmetric-key & public key cryptography. Although these systems have successfully proved their capability in securing information infrastructures (e.g., the Internet), many of them are found incompetent for wireless ad hoc networks, either due to severe communication or computing constraints, or due to the lack of infrastructure support in such networks.

1.1 MANET

Mobile Ad hoc Network consist of mobile nodes which can dynamically form a network to share information without using any pre-existing fixed infrastructure. Each node operates in distributed peer to peer mode & acts as a router & forward each other packets to enable information exchange between mobile hosts. In MANET, nodes are free to move and they can enter and exit from the network at any time. This leads to change in network topology frequently and unpredictably. Each node is equipped with radio interfaces that may have varying transmission/receiving capabilities. Each node carry batteries with limited power. Processing power of the mobile nodes is limited. MANETs can be applied

anywhere & any time, without any need of communication infrastructure. MANETs are applicable in Variety of fields including military battlefield, emergency/rescue operations in case of natural calamities i.e. floods, earthquake, fire etc.

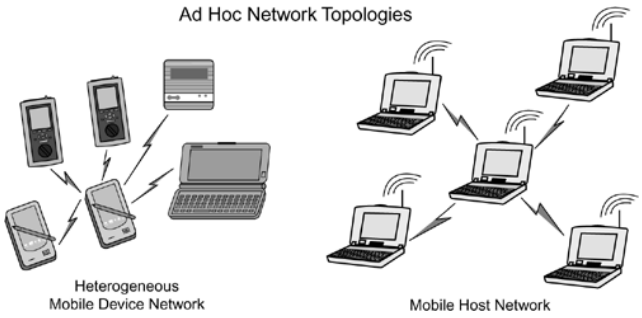

Figure 1: Heterogeneous mobile handheld devices and Mobile Ad hoc Networks.

1.2 Security in MANET

Security is a necessary service for wired and wireless network communications. The success of MANET strongly rely upon trust on the security. However, the characteristics of MANET offer both challenges and opportunities in attaining the security goals such as integrity, confidentiality, availability, access control, non-repudiation and authentication. Security is the combination of processes, procedures, and systems used to ensure integrity, confidentiality, availability, authentication, access control and non-repudiation [5].

- Confidentiality is to keep the information secret to unauthorized users or nodes. To keep information confidential, one way is to encrypt the message.
- Integrity means that the message can not be modified or destroyed in the transmission. When the data packet is sent through the wireless transmission medium, the block can be modified or deleted by malicious attacker nodes. The malicious attacker nodes can also resend it, which is called a replay attack.
- Authentication is to be able to identify a node or a user, and to be able to prevent impersonation. In infrastructure-based /wired wireless networks, it is possible to maintain a central authority at a point such as a base station or access point. But there is no central authority in ad hoc network, and it is much more difficult to authenticate an entity.
- Access control is to restrict unauthorized utilization of system resources and network services. Obviously, the access control is bind to authentication attributes. In general, access control is the most important service in both network communications and individual computer systems.
- Non-repudiation is associated to a fact that if an entity sends some information, the entity cannot deny that the message were sent by it. By adopting a signature for these message, the entity cannot later deny the data. In public key cryptography, a node A signs the packets using its private key. All other nodes can confirms the signed data packets by using A's public key. A cannot refuse the signature attached to the message.
- Availability is to keep the network resources or service available to legitimate users. It ensures the sustainability of the network despite malicious incidents.

Figure 2: The security trinity.

1.2.1 Security Issues and Challenges

In Wired Network, there are dedicated routers and security can be implemented on a centralized point whereas MANET have open peer to peer architecture [4]. Each mobile node acts as a router & forward packets for other nodes. The wireless channel is accessible to both authorize network user and malicious attackers. As a result, form security design viewpoint, there is no evident line of defence in MANET & there is no well-defined place/ infrastructure where single security solution may be applied. Moreover, restrictions in MANET resources pose another challenge in MANET security. The bandwidth of wireless channel is limited. The mobile nodes have limited computation and energy resources. Nodes are free to move, enter and exit the network at any time on their will. It creates dynamic network topology and increase the challenge in ensuring protected communication in hostile environment.

There are four main security problems that need to be dealt with in ad hoc networks [22]:

(1) The authentication of devices that want to talk to each other

(2) Setting up of secure session key among authenticated devices

(3) The secure storage of (key) data in the devices

(4) The secure routing in multi-hop networks [22].

1.2.2 Security Attacks

Security attacks can be categorized in different ways. One way is to divide attacks into four classes according to where the attacker deploys the attack in the flow of information from a source to a destination [22].

- Interruption: A network resource is destroyed or becomes unavailable or unusable. This attack is on availability. Examples include silently dropping control or data packets.
- Interception: An unauthorized node obtain access to an asset of the network. This is an attack on confidentiality. Examples include eavesdropping control or data packets in the networks.

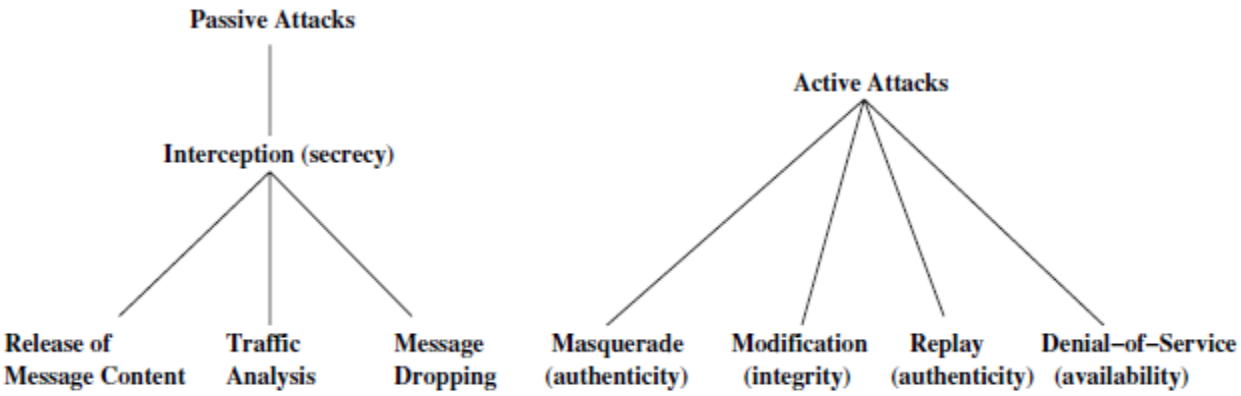

Figure 3: Categorization of Attacks**.**

- Modification: An unauthorized node not only obtain access to but modify the asset. This is an attack on integrity. Examples include modifying control or data packets [22].
- Fabrication**:** An unauthorized node inserts fake objects into the system. This is an attack on authenticity. Examples include inserting fake routing messages into the network or impersonating other node.

A more useful categorization of these attacks is in terms of active attacks & passive attacks [4]:

- Active attacks: An active attack involves alteration of the contents of messages or creation of false messages. It can be subdivided into four classes: modification of messages, replay attack, denial of service and masquerade [22].
- Passive attacks: A passive attack does not interrupt the working of a routing protocol, but only attempts to detect valuable information by eavesdropping. Three types of passive attacks are traffic analysis, release of message contents and message dropping.

1.2.3 Security mechanisms

Different security mechanisms have been devised to counter malicious attacks. The conventional approaches such as encryption, authentication, access control, and digital signature provide a first line of defence [4]. Intrusion detection systems and cooperation enforcement mechanisms implemented in MANET as a second line of defence. They can also help to defend against attacks & enforce cooperation, mitigating selfish node behaviour.

- Preventive mechanism: The conventional authentication and encryption methods are based on cryptography, which includes asymmetric and symmetric cryptography [5]. Public key cryptography approach depends upon centralized CA entity, which is a security weak point in MANET. Some authors propose to distribute CA functionality to multiple or all network entities based on a secret sharing scheme & some propose fully distributed trust model. Threshold cryptography can be used to hide data by breaking it into a number of shares Cryptographic primitives such as hash functions (message digests) can be used to improve data integrity in transmission as well. Digital signatures can be used to attain data integrity and authentication services as well. It is also essential to consider the physical safety of mobile devices, since the hosts are normally small devices, which are can be copped, lost, or damaged. The protection of the sensitive data on a physical device can be enforced by tokens or a smart card that is accessible through password, PIN or biometrics [4]. Although all of these cryptographic techniques combined can thwart most attacks in theory. In reality, due to the design, implementation, or selection of protocols and physical device limitation, there are still a number of malicious attacks that can detour prevention mechanisms.
- Reactive mechanism: The second line of defence is intrusion detection system [5]. The intrusion detection schemes for traditional wireless networks are not appropriate for MANET. There are widely used to detect misuse and anomalies. A misuse detection system keeps patterns of known attacks & by comparing them with the captured data, try to define improper behaviour, but it lacks the ability to detect any attacks that were not considered during the creation of the patterns. Anomaly detection attempts to specify normal or expected behaviour statistically. It collects data from authentic user behaviour over a period of time, and statistical tests are applied to determine anomalous behaviour with a high level of confidence. A variety of intrusion detection systems have been proposed by the researchers based on anomaly detection & misuse detection. Most of the proposed IDSs are distributed and have a cooperative architecture. In practice, both approaches can be used together to be more effective against attacks.

2. Related Work

In [6], Virender Pal Singh, Sweta Jain and Jyoti Singhai proposed a security framework for hello flood detection via signal strength and client puzzle method. Signal strength of all sensor nodes is assumed to be same in a radio range. Each node checks the signal strength of received hello messages with respect to the known radio range strength. Node is categorized as friend if they are same otherwise the sender node is categorized as stranger. Stranger node is checked for validity using some client puzzles. They use dynamic policy technique to adjust the difficulty level of puzzle for each node in terms of no. of hello messages sent. Higher the no. of hello message sent, higher the difficulty level of puzzles, it has to solve. It requires less computational power and energy.

In [7], Homgei Deng, Wei Li, and Dharma P. Agarwal proposed a method to surmount the black hole problem. The scheme assumes that every node that sends a RREP adds also the extra information of the next hop which allows the source to identify the replier's honesty. Therefore, when a source of a RREQ receives a RREP from an intermediate node the source sends an extra request called Further-Request to the next node and examine if the replier has actually a path to the destination. Due to the great overhead that the mechanism introduces the authors suggest its usage only in cases whenever the network finds a suspected node. The authors have not made any simulations of the mechanism's usage thus, factors such as detection time, false positive and false negative are not provided.

In [8], authors proposed a distributed and cooperative procedure to detect black hole node. In this each node discover local anomalies. It gathers information to create an estimation table which is maintained by each node. This table contains information regarding nodes in the power range. This scheme is started by the initial detection node which first broadcast and then it warns all one-hop neighbours of the possible suspicious node. They cooperatively decide that the node is suspicious node. Immediately after the confirmation of black hole, the global reaction is triggered to establish proper notification system to transmit warning to the whole network. The simulation result show the higher black hole detection rate and achieves better packet delivery. It achieves less overhead when the network is busier.

In [9], Satoshi Kurosawa et al proposes a new anomaly detection scheme based on dynamic learning process. It uses dynamic training method in which the training data is revised at regular time intervals. Multidimensional feature vector is defined to represent state of the network at each node. Each dimension is computed on every time slot. It uses destination sequence number to discover attack. The feature vector contain number of sent out RREQ messages, number of received RREP messages, the mean of difference of destination sequence number in each time slot between sequence number of RREP message and the one retained in the list. They compute mean vector by calculating some mathematical calculation. They match distance between the mean vector and input data sample. If distance is larger than some threshold value then there is an attack. The revised data set to be used for next detection. Anomaly detection is performed by repeating this for time interval T.

In [10], the authors discussed the two type of attack on ad-hoc network. The first on is Jelly Fish and second one is Black Hole attack. Significant progress has been made towards making ad hoc networks secure and DoS resilient. In this paper, the author develop the design and study DoS attacks in order to assess the damage that difficult-to-detect attackers can cause. Jellyfish attack, is targeted against closed-loop flows such as TCP. This attack is protocol-compliant and yet has a disastrous impact on the throughput of closed-loop flows, such as TCP flows and congestion-controlled UDP flows. These attacks are studied in a variety of settings and have provided a quantification of the damage they can inflict. As such a partitioned system is clearly undesirable, author also considered fairness measures and the mean number of hops for a received packet, as crucial performance measures for a system under attack. The main guidelines are provided for protocol designers who are creating DoS-resilience mechanisms, with a better understanding of the key attack factors and how to calculate the impact of an attack. Protocol designers can better decide if the overhead of deploying a counter-strategy is justified given the damage that an attack can make.

In [11], the author mainly discussed the malicious attacks on ad hoc networks. The main attacks which were identified are denial of service, changing the packet header, flooding packets and replaying and reordering data packets. Denial of service attacks include intentionally discarding packets instead of forwarding them and actively interfering in the communication of neighbouring nodes. Malicious nodes could alter the destination address of a data packet to reroute it. A malicious node could try to flood the network with its own unicast data packets, potentially using many different destination addresses. Malicious nodes can move to different areas of the network and replay data packets. Distance and node density affects the scope of an attack. Selection of routing protocol is based on the provision of security. Origin authentication & integrity mechanisms can be conventionally employed to proactive routing, as the control packets used are not altered as they move through the ad hoc network. Even though reactive routing protocols may provide substantial gains in saving resource to proactive routing, they are more complex and may also be more difficult to secure.

In [12], authors proposes Cross layer Active RE-routing (CARE) for MANETs. It detects attacks at the transport layer but reacts to them at the network layer. CARE is composed of two modules: the congestion window monitoring (CWM) module and the least-alike re-routing (LAR) module. CWM is accountable for detecting any abnormalities that might occur on a route. LAR module execute re-routing at the network layer. CARE is designed to thwart a wide range of attacks including black hole, worm hole, gray hole, jelly fish and rushing attacks. CARE is effective in mitigating JF attacks in certain network environments.

In [13], authors deign and evaluate Secure Efficient Distance vector routing protocol (SEAD) for Mobile Wireless Ad Hoc Networks. This is based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV). In order to support use nodes having restricted CPU processing capability and to guard against Denial-of-Service (DoS) attacks, this uses efficient one-way hash functions. It does not use asymmetric cryptographic operations in the protocol. This is robust scheme against many uncoordinated attackers generating incorrect routing state in any other node, even in spite of active attackers or compromised nodes in the network. It can be used in networks having computation and bandwidth constrained nodes.

In [14], authors propose a scheme for detection and isolation of misbehaving nodes based on sending acknowledgement packets for reception of data packets. Their approach uses promiscuous mode for counting the no

of data packets such that it overcomes the problem of misbehaving nodes. In the proposed approach, each node maintains a LIST which consist of ID of every data packet sent or forwarded. LNode of every group will make an entry of forwarded data packet in the list and wait for ACK-1 and ACK-2 packet which are communicated from Rnode of first set and Rnode of second set respectively. Also ACK-1 and ACK-2 packets must be received within time T1 and Time T2 respectively. Proposed approach can be integrated on top of any source routing protocol such as DSR. The proposed approach has routing overhead.

In [15], authors summarize that Transmission Control Protocol (TCP) is a transport layer protocol which provides flow control, congestion avoidance and error control. TCP is designed to provide the reliable end to end byte stream communication and little or almost no consideration was given to the fact that algorithms used in TCP can be exploited by attackers while designing this protocol. Low rate TCP-targeted denial of service attack is a cleverly crafted attack in which an attacker make use of congestion avoidance algorithm and uniformity of minimum Retransmission Time out period in Transmission Control Protocol. Optimistic acknowledgement for any misbehaving TCP receiver is suggested for detection and mitigation of Induced Low rate TCP-targeted attack. This solution mitigates this Induced Low rate TCP-targeted attack by stopping optimistic acknowledgement.

In [16], authors designed a lightweight security scheme to detect and prevent disassociation DoS attacks to satellite networks. In such a disassociation DoS attack, the attacker can sniff the sending packet and generate a bogus disassociation request to the network control centre (NCC), with aim to prevent legitimate users from accessing the service. Based on the characteristics of the one-way Rabin function, the proposed solution has employed the Rabin function to encrypt the sequence number in order to improve the security of the sequence number. The authors provide preliminary modelling verifications and simulation results related to efficiency and practicability of this new approach. Through the analysis of the simulation results, the proposed method is found to be able to efficiently prevent DoS attacks and have low consumption of computation resources by avoiding further verification.

V. Geetha et al. [17], propose a parameter and trust factor based secure communication framework and design a trust management system for wireless sensor networks. The trust of a neighbour node is calculated based on evaluation of trust factors. Each trust factor is computed based on observed parameters. To calculate trust between two nodes, a node has to observe its neighbour for its interactions with node. The authors have identified total six groups of data to be observed on the network. The results are analysed for 10%, 20% and 30% attacker nodes. The metrics used for comparison of results is based on True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). The results are measured against standard Bayesian trust model (STM) with exponential decrease Bayesian trust model (ETM). The simulation results in MATLAB prove that the proposed model works for secure communication, data aggregation and intrusion detection in wireless sensor networks.

Asma et. al [19] presented a trust based solution for securing the OLSR Ad Hoc routing protocol. In the first step, they analyse the implicit trust relations in OLSR. In the second step, they developed trust-based reasoning by correlating information provided in OLSR messages received from the network. The third step offers prevention to resolve certain vulnerabilities of OLSR and countermeasures to stop and isolate malicious nodes.

Shuaishuai et. al. [20] proposed FPNT-OLSR, a trust reasoning model based on fuzzy Petri net which evaluate trust values of mobile nodes. They also propose a trust based routing algorithm to select a path with the maximum path trust value among all possible paths. For implementation of FPNT-OLSR, they designed a trust factor collecting method and efficient trust information propagation method, which do not generate extra control messages.

Sanjeev et. al [21] proposed a security mechanism which defend external attack as well as ensures secure routing by permitting only those routes which include trusted node. Authenticity and integrity of non-mutable and mutable fields of control message is ensured by digital signatures and hash chain. A field THNA (Two hop Neighbour Authentication) Ticket is appended in HELLO and TC Message Extension Format. If node A wishes to authenticate node B then it follows the steps of mutual authentication between two nodes. They exchange THNA as the proof of their relationship. Both nodes verify the link status by validating their THNAs. MPR selection will be done after verification success. Timestamp exchange process is introduced to add freshness in the message and to foil replay attacks by using control messages.

3. Proposed Methodology

Mobile Ad hoc Networks (MANET) is new paradigm of wireless networks providing unrestricted mobility to nodes with no fixed or centralized infrastructure. Each node participating in the network acts as router to route the data from source to destination. This characteristic makes MANET more susceptible to routing attacks. The various authors have given various proposals for detection and prevention of DoS attack in MANET but every proposal has some limitations. We proposed a trust mechanism along with robust random early detection mechanism to isolate three different DDOS attacks over considered scenarios.

Algorithm: A Proposed Mechanism for NODE's Trust value calculation.

1. T (i) – Trust value of Node i
2. T (j) – High Trusted MPR neighbor
3. Tx - Transmission range and
   R_{xy} - Route from node i to node j
4. If ($R_{xy} < Tx$) and route is consistent (1 hop) {
5. Node i and Node j are neighbors
6. Node i send directly to Node j.
7. } else MPR – Multipoint Relay selection part
8. If (a node receiver of the route msg from a MPR and it has sent the message to network -broadcast) then

9. If the information in the route msg is consistent then
10. If (secondary rating of the MPR in its rating table > Primary rating of the MPR in its rating table) then
11. Primary rating = Primary Rating+2/3(Secondary Rating - Primary rating)
12. Secondary Rating = Secondary Rating + Primary Rating;
13. MPR =T (i)
14. Else
15. Primary rating = secondary rating and secondary rating = secondary rating -2;
16. End;

As per earlier discussion, simulation is performed using ns-2 simulator to analyse and evaluate the effect of three DoS attack on OLSR routing protocol under different pause time scenarios. Here, this performance is evaluated based on different performance metrics like throughput, and packet delivery ratio. A detail simulation study is presented below.

Table 1: Important Simulation Parameters

Parameter	Value
Simulation area	1600m x 500m
Antenna	Omni antenna
No. of nodes	30
Pause Time (sec)	5, 10, 15, 20, 25, 30
Packet size	512 Bytes
Max queue length	50
Traffic	CBR (Constant bit rate)
Routing protocol	OLSR
Attack Type	Spoofing attack, Route flooding and HELLO flooding
Defence Mech.	NODE's Trust Mechanism along with RRED.

Throughput

The figure 2 shows the throughput of OLSR under three different DDOS attack for various pause times. The figure depicts that throughput of OLSR routing protocol is heavily affected by spoofing attack than other flooding attack.

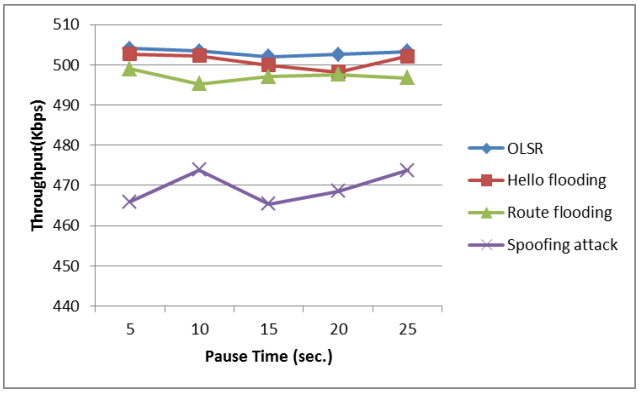

Figure 4: Throughput of OLSR along with three different DDOS attacks.

The figure 3 shows the throughput of OLSR under proposed scheme along with RRED policy gives better results and isolated most of the flooding. This figure confirms that the throughput is much improved while QoS policy namely RRED and Proposed Trust assignment schemes are used against HELLO flooding attack.

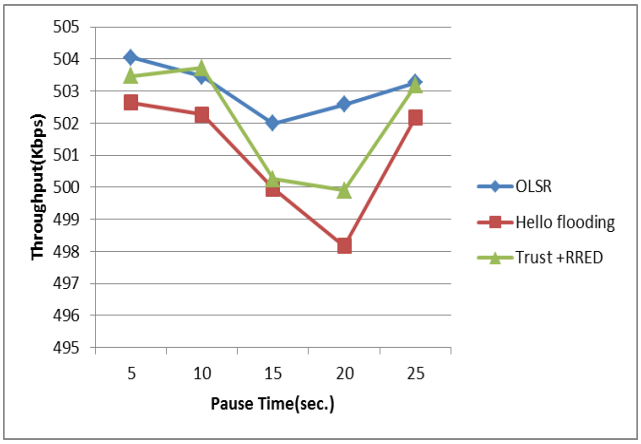

Figure 5: Throughput of OLSR along with Hello flooding attack and their isolation schemes.

The figure 4 shows the throughput of OLSR under route Flooding DDOS attack and Proposed Trust assignment and QoS RRED policy.

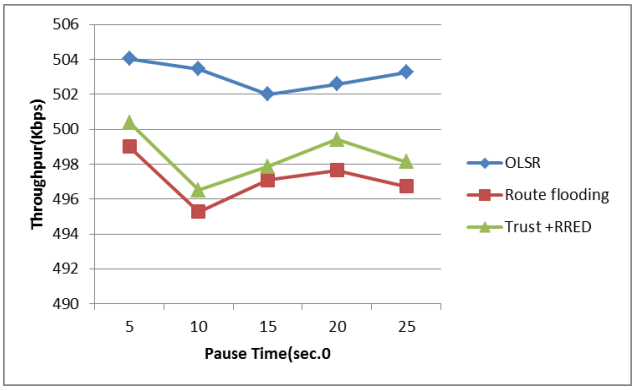

Figure 6: Throughput of OLSR along with Route flooding attack and their isolation schemes.

The figure 5 shows the throughput of OLSR under Spoofing DDOS attack and Proposed Trust assignment and QoS RRED policy.

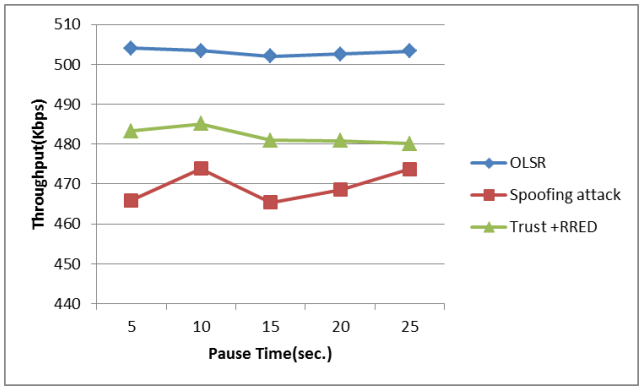

Figure 7: Throughput of OLSR along with spoofing attack and their isolation schemes.

Packet Delivery Fraction (PDF)

Figure 6 shows the packet delivery ratio when the pause time is varied.The figure depicts that throughput of OLSR routing protocol is heavily affected by Spoofing attack than other flooding attacks.

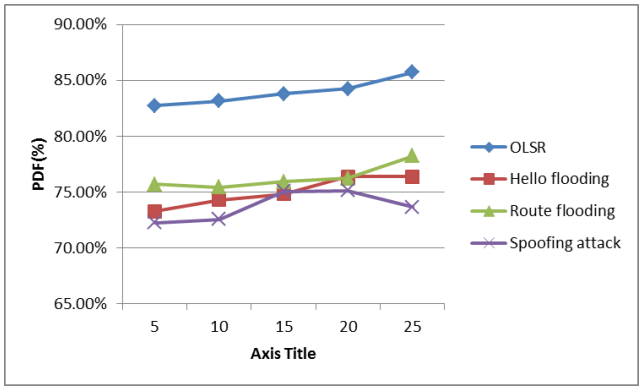

Figure 8: PDF of OLSR along with three different DDOS attacks.

The figure 7 shows the PDF of OLSR under hello flooding for different pause time. This figure confirms that the PDF of OLSR routing protocol is improved while combination of QoS policy namely RRED and Proposed Trust assignment scheme against low hello flooding attack.

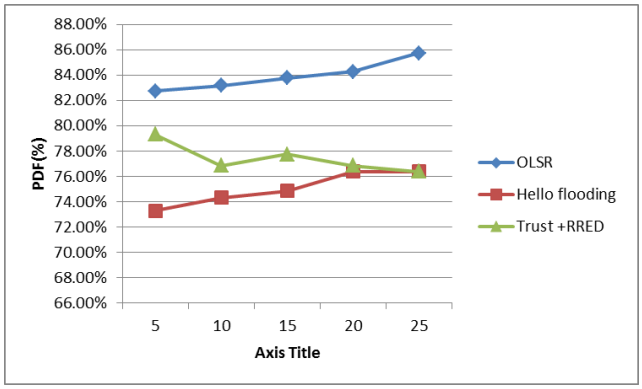

Figure 9: PDR of OLSR along with Hello flooding attack and their isolation schemes.

The figure 7 shows the PDF of OLSR under Route flooding attack and its isolation using proposed combination of trust and QoS policy for varying pause time. This figure confirms that the PDF of OLSR routing protocol is improved while proposed trust scheme along with QoS policy used against route flooding attack.

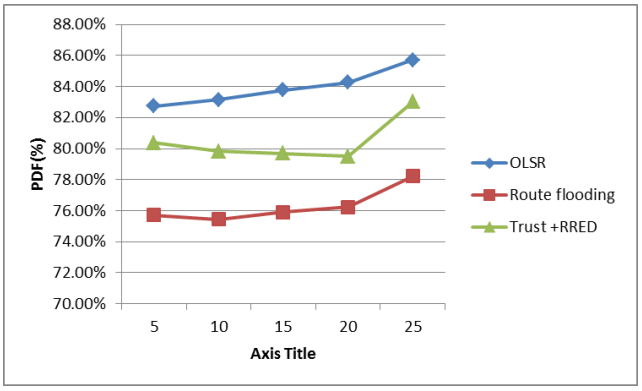

Figure 10: PDR of OLSR along with Route Flooding attack and their isolation schemes.

The figure 9 shows the PDF of OLSR under Spoofing DDOS attack and Proposed Trust assignment and QoS RRED policy.

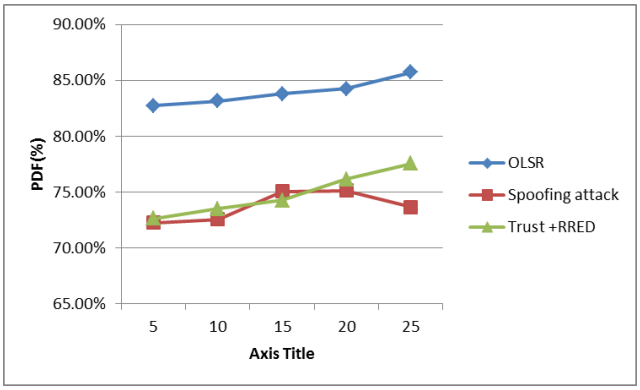

Figure 11: PDR of OLSR along with spoofing attack and their isolation schemes.

4. Conclusion and Future Work

In this paper, we simulated three different types of DDoS attacks against OLSR routing protocol in Wireless Ad hoc Networks and investigated its affects. Simulation results shows that spoofing attack heavily affects the overall network performance as compare to route flooding attack. Although many solutions have been proposed for flooding attacks and spoofing schemes but still these solutions are not perfect in terms of effectiveness and efficiency. Our proposed solution tries to reduce the effect of flooding and spoofing attacks by using trust evaluation of route before forwarding it to neighboring MPR station, along with QoS cache management scheme that tries to prevent and notify the other nodes regarding congestion area to optimize the working of OLSR routing algorithm. Simulation results shows that proposed `schemes efficiently isolate these flooding and spoofing attacks and increase the overall network performance.

5. References

[1] C.S.R Murthy, B.S. Manor, “Ad Hoc Wireless Networks Architectures and Protocols”, Prentice Hall PTR, 2004

[2] T. Clausen, P. Jacquet, IETF RFC-3626: Optimized Link State Routing Protocol OLSR, 2003.

[3] I. Noman and Z.A. Saokh, “Security Issues in Mobile Ad Hoc Network”, Wireless Networks

and Security, Springer Berlin Heidelberg, pp 49-80, 2013

[4] Farooq Anjum, Petros Mouchtaris, "Security for Wireless Ad Hoc Networks", Wiley 2007.

[5] Erdal Cayirci, Chunming Rong, "Security in Wireless Ad Hoc and Sensor Networks", Wiley 2009.

[6] Virendra Pal Singh, Sweta Jain and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", International Journal of Computer Science Issues, Vol. 7, Issue 3, No. 11, May 2010, pp 23 – 27.

[7] Hongmei Deng, Dharma P. Argawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, October 2002.

[8] Chang-Wu Yu, Tung-Kuang Wu, Rei-Heng Cheng, Kun-Ming Yu, Shun Chao Chang: A Distributed and Cooperative Algorithm for the Detection and Elimination of Multiple Black Hole Nodes in Ad Hoc Networks. IEICE Transactions 92-B (2), 483-490 (2009).

[9] Nakayama, H., Kurosawa, S., Jamalipour, A., Nemoto, Y.; Kato, N., "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks," *Vehicular Technology, IEEE Transactions on* , vol.58, no.5, pp.2471,2481, Jun 2009.

[10] Imad Aad, Jean-Pierre Hubaux, Edward W. Knightly , "Impact of Denial of Service Attacks on Ad Hoc Networks, " IEEE/ACM transactions on networking, VOL. 16, NO. 4, pp no 791-802, August 2008.

[11] Po-wah yau, Shenglan hu and Chris j. Mitchell, "Malicious attacks on ad hoc network routing protocols", ACM student magazine, 2005.

[12] Ruiliang Chen, Jung-Min Park, and Michael Snow, "CARE: Enhancing Denial-of-Service Resilience in Mobile Ad Hoc Networks", Proceedings 15th International Conference on Computer Communications and Networks, ICCCN 2006, pp no 5 – 10, 9-11 Oct. 2006

[13] Yih-Chun Hu, David B. Johnson, Adrian Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks" SciencDdirect, vol 1, issue 1, pp no 175-192, July 2003.

[14] Aishwarya Sagar Ananad Ukey and Meenu Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", International Journal of Computer Science Issues, Vol. 7, Issue 4, No. 1, July 2010, pp 12 – 17.

[15] Ferdous A. Barbhuiya, Vaibhav Gupta, Santosh Biswas and Sukumar Nandi, "Detection and Mitigation of Induced Low Rate TCP-Targeted Denial of Service Attack" IEEE Sixth International Conference on Software Security and Reliability, Oct. 2012.

[16] Ting Ma, Yee Hui Lee, Maode Ma, "Protecting Satellite Systems from Disassociation DoS Attacks" Wireless Personal Communication, Springer, pp. 623–638, March 2012.

[17] V. Geetha and K. Chandrasekaran, "A Distributed Trust Based Secure Communication Framework for Wireless Sensor Network" Wireless Sensor Network, scientific research, 2014, pp. 183-183.

[18] Aleksandar Kuzmanovic and Edward W. Knightly, "Low Rate TCP Targeted Denial of Service Attacks" *SIGCOMM'03,* August 25-29, 2003.

[19] Asma Adane, Christophe Bidan, Rafael Timoteo de Sousa Junior, "Trust based security for the OLSR protocol", Computer Communications, Elsevier, 2013.

[20] Shuaishuai Tan, Xiaoping Li, Qingkuan Dong, "Trust based routing mechanism for securing OLSR based MANET", Journal of Ad Hoc Network, Volume 30, Issue C, July 2015, pp 84-98.

[21] Sanjeev Kumar Rana and Arun Kapil, "Defending Against Node Misbevior to Discover Secure Route in OLSR", Proceedings of International Conference on Business Adminintartion and Information Processing (BAIP-2010), Springer Verlag Berlin Heidelberg, CCIS 70, pp 430-436, 2010.

[22] Yang Xiao, Xuemin Shen, Ding-Zhu Du, "Wireless Network Security", Springer Science & Business Media, 2007.

First Author Suveg Moudgil is working as an Asso. Professor, Department of Computer Engineering, H.E.C, Jagadhri. He obtained his B. Tech. & M. Tech. (Computer Engineering) from Kurukshetra University, Kurukshetra. He is doing Ph. D (Computer Engineering) from M. M. U., Mullana, Ambala. He has experience of 15 years. He has a no. of publications in international journals/conferences to his credit. His research areas include wireless communication, mobile ad hoc networks, sensor based networks and network security etc.

Second Author Dr. Sanjeev Rana is working as Professor at MMEC, M. M. University, Mullana, Ambala. He obtained his Ph. D (Computer Engineering) from M. M. U., Mullana, Ambala. He is CISCO certified instructor. He has teaching experience of more than 16 years. He has more than 30 publications in various international journal/conferences to his credit. He has guided 15 M. Tech. Students. Currently, He is supervising three Ph. D research scholars. His current research interest include network security, operating systems, wireless communications, mobile ad hoc networks and sensor based network.