Securing MANET from jellyfish attack using selective node participation approach

Arminder Kaur, Dr. Tanu Preet Singh

***Abstract*— Mobile ad hoc networks (MANETs) are highly vulnerable as there is no presence of trusted centralized authority and dynamic network topology. Due to such characteristics of MANET various kind of attacks are possible. Jellyfish (JF) is a new denial of service attack. The goal of jellyfish node is to diminish the good put, which can be achieved by dropping some of packets. In this paper we have proposed a secure technique in TORA protocol using selective node participation approach to diminish the impact of Jellyfish attack in MANET. The selective node participation approach identifies JF nodes during route creation and assigned it as an inactive and selects a subset of nodes to participate as part of the network.**

***Index Terms*— MANET, Jellyfish Attack, AODV, DSR, TORA, TCP.**

I. INTRODUCTION

MANET contains mobile nodes, communicating in a multihop manner without any fixed infrastructure i.e, access points. A malicious attacker can easily access this kind of network because of the lack of strong defence mechanism and high mobility of nodes. Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority, lack of trust relationships between mobile nodes, easy eavesdropping because of shared wireless medium, dynamic network topology, low bandwidth, and battery and memory constraints of mobile devices. Among all the research issues, security is an essential requirement in MANET environments. Jellyfish is a new denial of service attack that exploits the end to end congestion control mechanism of TCP (Transmission Control Protocol) which has a very devastating effect on the throughput. The Jelly fish attacker nodes fully obeys protocol rules, hence this attack is called as passive attack. Due to JF attack, high end to end delay takes place in the network.

II. JELLYFISH ATTACK

Jellyfish attacks work on MANETs that use protocols with congestion control techniques, such as the Transmission Control Protocol (TCP), in the transport layer. JF attacker needs to intrude into forwarding group and then it delays data packets unnecessarily for some amount of time before forwarding them. Due to JF attack, high end to end delay takes place in the network. So the performance of network (i.e. throughput etc) decreases substantially. JellyFish attack is divided into three categories- JF Reorder Attack, JF Periodic Dropping Attack, JF Delay Variance Attack.

A. Jellyfish Reorder Attack

In this attack JF nodes maliciously re-order packets. In this attack, JF deliver *all* packets, yet after placing them in a re-ordering buffer rather than a First In First Out (FIFO) buffer. Consequently, we will show that such persistent re-ordering of packets will result in near zero goodput, despite having all transmitted packets delivered.This attack is possible due to well known vulnerability of TCP. Jelly fish attacker uses this vulnerability to record packets. This is possible because of factors such as route changes or the use of multipath routing.[4]

B. Jellyfish Periodic Dropping Attack

The JF Periodic dropping attacking nodes drop all packets for a short duration (e.g., tens of ms) once per Retransmission Time Out (RTO). Periodic dropping is possible because of sarcastically chosen period by the mischievous node. This kind of periodic dropping is possible at relay nodes. Suppose that congestion losses force a node to drop a% of packets. Now consider that the node drops a% of packets periodically then TCPs throughput may be reduced to near zero even for small values of a [4].These attacks exploit a weakness in TCP which means that if packet losses occur periodically near the RTO time-scale, then end-to-end throughput is almost reduced to zero.

C. JF Delay Variance Attack

In this type of attack, the malicious node randomly delays packet without changing the order of the packets [4] and then it delays data packets for some amount of time before forwarding. Due to JF delay variance attack, high end- to- end delay takes place in the network and performance of the network (i.e. throughput etc) becomes worse. High delay variation can cause TCP to send traffic in bursts due to "self-clocking," which leads to increase collisions and loss. It also causes misestimations of available bandwidth. High delay variation leads to an excessively high Retransmission time out (RTO) value. Packets delayed by the JF attacker have the potential to significantly reduce throughput of network. Intruder (JellyFish) node waits for a variable amount of time before forwarding each packet. They maintain FIFO order of packets, but significantly increase delay variance.[3]

III. TEMPORALLY- ORDERED ROUTING ALGORITHM

TORA perform three operations such as Route Creation, Route Maintenance and Route Erasure. The creating routes operation is responsible for selecting proper heights for routers and forming a directed sequence of links leading to the destination in a previously undirected network.[9] The

Manuscript received April 07, 2015.

Arminder Kaur, Department of Electronics & Communication, Amritsar College of Engineering & Technology, Amritsar, Punjab, India.
Dr. Tanu Preet Singh, Department of Electronics & Communication, Amritsar College of Engineering & Technology, Amritsar, Punjab, India.

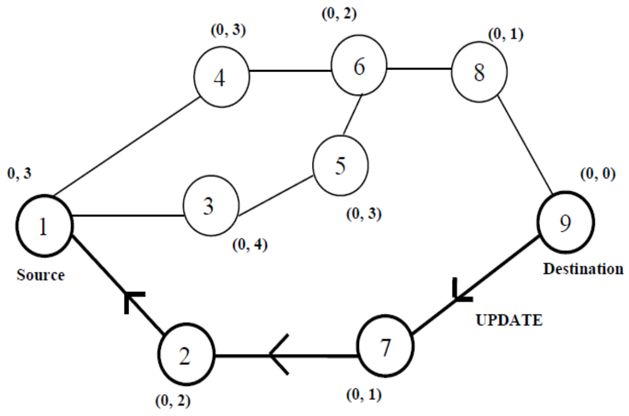
maintaining routes procedure is the operation that responds to network topology changes. The operation of erasing routes is used to set routers' heights to NULL and set links to undirected. It maintain [17] at least one route to destination in the routing tables. The initiation of route searching happens only when the source wants to send data packets to the destination.[14]

Three packets are used to perform these operations:

- QUERY (QRY),
- UPDATE (UPD),
- CLEAR (CLR)

Initially to create a route, the node broadcasts a QUERY packet to its neighbors. This QUERY is re-broadcasted through the network until it reaches the destination or an intermediate node that has a route to the destination. The recipient of the QUERY packet then broadcasts the UPDATE packet which lists its height with respect to the destination. When this packet propagates in the network, each node that receives the UPDATE packet sets its height to a value greater than the height of the neighbor from which the UPDATE was received. This has the effect of creating a series of directed links from the original sender of the QUERY packet to the node that initially generated the UPDATE packet. When a node discovers that the route to a destination is no longer valid, it will adjust its height so that it will be a local maximum with respect to its neighbors and then transmits an UPDATE packet. If the node has no neighbors of finite height with respect to the destination, then the node will attempt to discover a new route.[20]

As shown in fig.1, node 6 does not propagate QUERY from node 5 as it has already seen and propagated QUERY message from node 4 and the source may have received a UPDATE each from node 2, it retains that height. When a node detects a network partition, it will generate a CLEAR packet that results in reset of routing over the ad hoc network. The establishment of the route is based on the DAG mechanism thus ensuring that all the routes are loop free. Packets move from the source node having the highest height to the destination node with the lowest height like top-down approach.



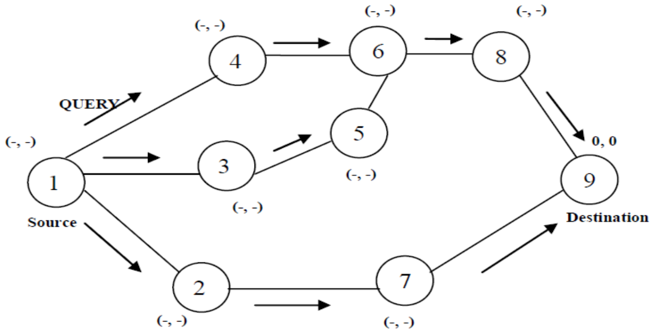


Figure.1 Route creation in TORA

IV. PROPOSED ALGORITHM

The proposed work is a technique that will optimize the impact of Jellyfish attack in MANET by selective node participation approach. This approach implements the following features:

• A *node status* variable stored in nodes (with respect to a particular destination) that states whether it participates as part of the network.

• A *probability active* constant that determines the probability that a node is assigned an active status.

The nodes are assigned either an active, inactive, or unassigned status. All nodes are given an unassigned status when they first boot up. During route creation, a node propagates QRY packets when it requires a route to a destination. When a node *i* receives a QRY packet, it performs as follows:

1) If the QRY packet is processed as per normal flow, *node status* is active.
2) If the QRY packet is delayed for 0 to 10 sec, *node status* is inactive.
3) If *node status* is unassigned and one of its neighbor is the destination or source, *node status* is set as active and the QRY packet broadcast.
4) If *node status* is unassigned and none of its neighbor is the destination or source, *node status* is randomly set as active or inactive according to *probability active and* the QRY packet is broadcast if the *node status* assigned is active.

The flooding of QRY packets sets *node status* in all nodes to either active or inactive. This reduces the QRY packets propagated compared to original TORA since nodes assigned an inactive status no longer propagate QRY packets. The optimal value for *probability active* is dependent on the node density and mobility of the network. A high *probability active* value makes it perform like original TORA while a low value creates unnecessary network partitions.

Fig. 2(b) gives an example of how a network is initialized using the selective node participation approach in the presence of JF attack. The initially uninitialized network where node 1 requires a route to node 20. After route creation using the selective node participation approach, we obtain an initialized network (Fig 1(b)) where the nodes assigned a *node status* of active (yellow) participate as part of the network. JF Nodes that are assigned a *node status* of inactive (maroon) do not participate thus reducing impact of Jellyfish Attack. At the same time, there still exists multiple routes from node 1 to 20.

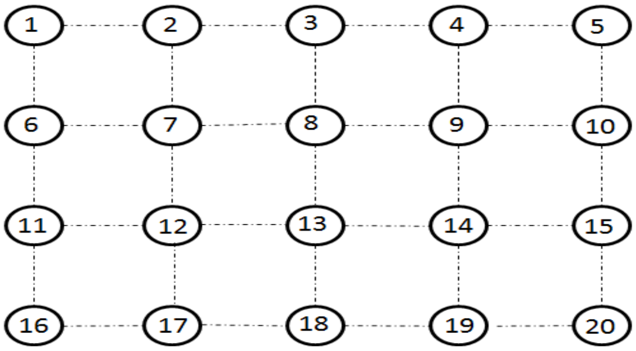


Figure.2 (a) The initially uninitialized network where node 1 requires a route to node 20.

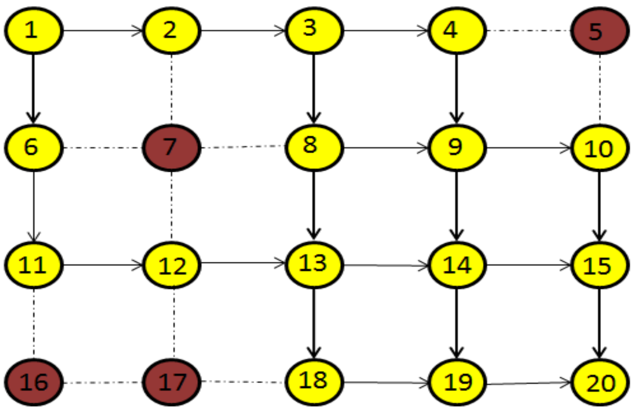


Figure. 2(b) Using Selective Node Participation Approach, JF nodes are assigned a node status of inactive do not participate in routing thus reducing the impact of JF attack. At the same time, there still exists multiple routes from node 1 to 20.

V. PERFORMANCE METRICS

A. Packet Delivery Ratio (PDR)

PDR is the ratio of data packets delivered to the destination to those generated by the sources.[1] It is calculated as follow:

$$\mathrm{PDR} = \frac{Number\ of\ Packets\ Recieved}{Number\ of\ Packets\ Sent} * 100 \qquad (1)$$

B. Throughput (TP)

Average TP is the number of bytes received successfully [1] and it is calculated as follow:

$$\mathrm{TP} = Number\ of\ Bytes\ Received * 8 * Simulation\ Time * 1000kbps$$
(2)

C. End-to-End Delay (e2e delay)

Average e2e delay is the average time of the data packet to be successfully transmitted across the network from source to destination. It includes all possible delays such as buffering during the route discovery latency, queuing at the interface queue, retransmission delay at the MAC, the propagation, and the transfer time [1]. The average e2e delay is computed as follow:

$$\mathrm{e2e\ delay} = \textstyle\sum_{i=1}^{n} (\mathrm{Ri} - \mathrm{Si})/\mathrm{n} \qquad (3)$$

Where n is the number of data packets successfully transmitted over the network, i is the unique packet identifier, Ri is the time at which a packet with a unique identifier i is received and Si is the time at which a packet with a unique identifier i is sent.

VI. SIMULATIONS AND RESULTS

The simulations were performed using Network Simulator 2 (Ns-2), particularly popular in the ad hoc networking community. *Ns-2* is a discrete event simulator that allows for the modelling of a variety of protocols over wired, wireless and satellite networks. The mobility model used is Random Way point Model. The traffic sources are CBR (continuous bit –rate), data packet size is 64 bytes and data sending rate is 4 packet/second. During the simulation, each node starts its journey from a random spot to a random chosen destination. Once the destination is reached, the node takes a rest period of time in second and another random destination is chosen after that pause time. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. The simulation time is 900 seconds and maximum speed of nodes is 1 m/s. The following scenario is used in this paper

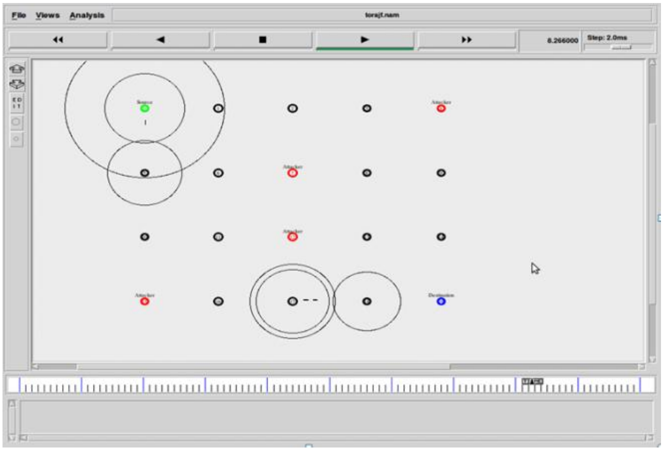


Figure 3. MANET under Jellyfish Attack (20 nodes)

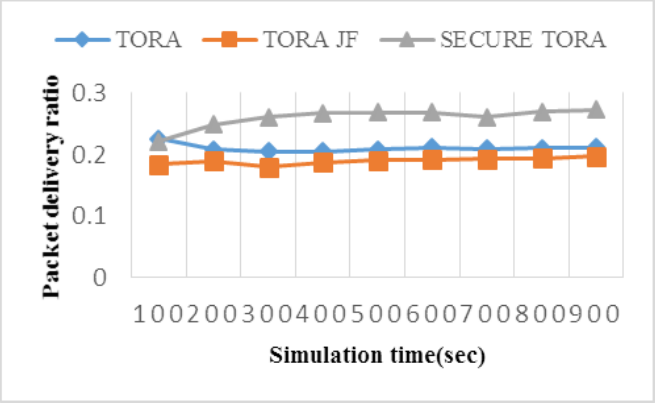


Figure 4. Packet Delivery Ratio

Figure 4 shows Packet Delivery Ratio with normal flow (zero attackers, TORA), in the presence of JF attackers (TORA JF) and in the presence of JF attackers with selective node participation approach (SECURE TORA).

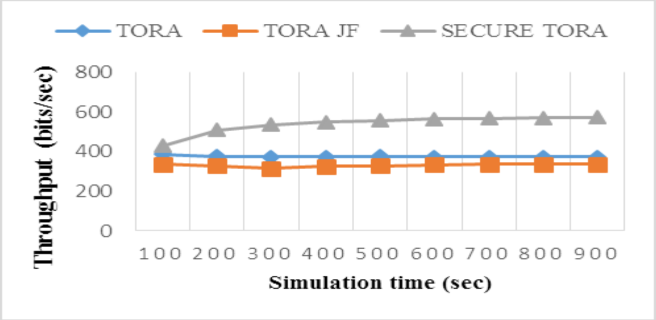


Figure 5. Throughput(s)

Figure 5 shows Throughput with normal flow (zero attackers, TORA), in the presence of JF attackers (TORA JF) and in the presence of JF attackers with selective node participation approach (SECURE TORA).

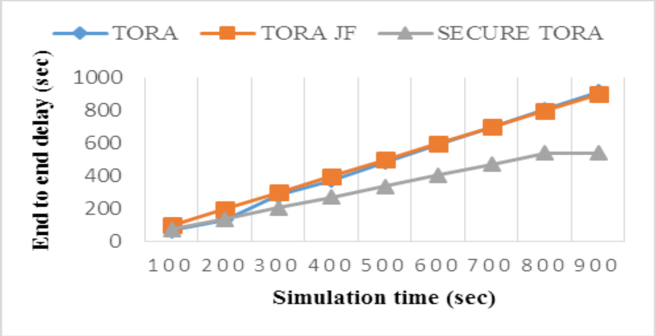


Figure 6. End to end delay(s)

Figure 6 shows End to end delay with normal flow (zero attackers, TORA), in the presence of JF attackers (TORA JF) and in the presence of JF attackers with selective node participation approach (SECURE TORA).

VII. CONCLUSION

This paper presents the impact of JF attack on MANET using normal TORA and using the proposed Selective Node Participation Approach. The proposed approach reduces the impact of JF attack in MANET by deactivating the JF nodes to participate in the DAG but still maintain the overall integrity of the DAG. It has been concluded that the performance of network has been improved by Selective Node participation in terms of End to end delay, Packet Delivery Ratio and Throughput of the network.

VIII. FUTURE SCOPE

Here we have taken JF Delay Variance attack, we can also introduce some other kind of JF attack i.e. JF Reorder Attack and JF Periodic Dropping Attack in the same scenario. We take mobility and system size as constant, if we change these two factors then performance may vary. So this work can be further extended to calculate the performance of MANET under varying mobility and system size.

REFERENCES

[1] Lamyaa M.T. Harb, Dr. M. Tantawy, NTI, and Prof. Dr. M. Elsoudani, " PERFORMANCE OF MOBILE AD HOC NETWORKS UNDER ATTACK", 2013 IEEE.

[2] Amandeep Kaur, Deepinder Singh Wadhwa, "Effects of Jelly Fish Attack on Mobile Ad-Hoc Network's Routing Protocols", International Journal of Engineering Research and Applications, ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.1694-1700.

[3] Mohammad Wazid, Vipin Kumar, RH Goudar, "Comparative Performance Analysis of Routing Protocols in Mobile Ad Hoc Networks under Jelly Fish Attack," 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[4] Mr. Hepikumar r. Khirasariya, "Simulation study of jellyfish attack in manet (mobile ad hoc network) using AODV routing protocol", journal of information, knowledge and research incomputer engineering, issn: 0975 – 6760| nov 12 to oct 13 | volume – 02, issue – 02.

[5] Hoang Lan Nguyen, Uyen Trang Nguyen, "A STUDY OF DIFFERENT TYPES OF ATTACKS IN MOBILE AD HOC NETWORKS", 2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE).

[6] Jan von Mulert, Ian Welch , Winston K.G. Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV", Journal of Network and Computer Applications 35 (2012) 1249–1259.

[7] Hui Lim and Amitava Datta, "Enhancing the TORA Protocol using Network Localization and Selective Node Participation," 2012 IEEE.

[8] Kwan Hui Lim and Amitava Datta, "An In-depth Analysis of the Effects of IMEP on TORA Protocol," 2012 IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks.

[9] Er.Punardeep Singh, Er.Harpal Kaur, Er. Satinder Pal Ahuja," Brief Description of Routing Protocols in MANETS And Performance And Analysis (AODV, AOMDV, TORA)", International Journal of Advanced Research in Computer Science and Software Engineering (IJARSSE), Volume 2, Issue 1, January 2012.

[10] Nidhi Purohit, Richa Sinha, Hiteishi Diwanji, Simulation Study of Black Hole and Jellyfish attack on MANET Using NS3", Special Issue of International Journal of Computer Applications (0975 – 8887) on Wireless Communication and Mobile Networks, No.9. Jan.2012, ww.ijcaonline.org.

[11] Syed Atiya Begum, L.Mohan, B.Ranjitha, "Techniques for Resilience of Denial of Service Attacks in Mobile Ad Hoc Networks", International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X,2012.

[12] Jun-Won Ho , Matthew Wright , Sajal K. Das, "Distributed detection of mobile malicious node attacks in wirelesssensor networks", science direct journal, Ad Hoc Networks 10 (2012) 512–523.

[13] Ashok M.Kanthe, Dina Simunic and Marijan Djurek, "Denial of Service (DoS) Attacks in Green MobileAd–hoc Networks", MIPRO 2012/CTI.

[14] Imad Aad, Jean-Pierre Hubaux, Edward W. Knightly, "Impact of Denial of Service Attacks on Ad HocNetworks", IEEE.

[15] Rajeswari.M, Dr.P.Uma Maheswari, Bhuvaneshwari.S,Gowri.S, "Performance analysis of AODV, DSR, TORA and OLSR to achieve group communication in MANET," IEEE- Fourth International Conference on Advanced Computing, ICoAC 2012 MIT, Anna University, Chennai. December 13-15, 2012.

[16] G.Pragadeeswaran, D.Ezhilarasi, P.Selvakumar," A Performance Analysis of TORA, AODV and DSR Routing Protocols in MANET using NS2", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012, Issue 6, June-2012.

[17] Puneet Dadral, Rajan Vohra, Ravinder Singh Sawhney, "Metrics Improvement of MANET Using Reactive Protocols Approach," 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[18] Mina Vajed Khiavi, Shahram Jamali, Sajjad Jahanbakhsh Gudakahriz, "Performance Comparison of AODV, DSDV, DSR and TORA Routing Protocols in MANETs," International Research Journal of Applied and Basic Sciences. Vol., 3 (7), 1429-1436, 2012.

[19] Ashish Kumar Jain, Vrinda Tokekar, "Classification of Denial of Service Attacks in Mobile Ad Hoc Networks", 2011 International Conference on Computational Intelligence and Communication Systems,IEEE Computer Society 2011.

[20] Eiman Alotaibi, Biswanath Mukherjee, "A survey on routing algorithms for wireless Ad-Hoc and mesh networks", science direct journal, Computer Networks 56 (2012) 940–965.

[21] Tushar J. Raval, J.S. Shah, "Network Density Based Analysis of Geographic Routing Protocol for Random Mobility of Nodes in MANET," 2011 IEEE.

[22] R. Sudha, Dr. D. Sivakumar, "A Temporal table Authenticated Routing Protocol for Adhoc Networks," 2011 IEEE.

[23] G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in MANETS", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010.

[24] V. PALANISAMY, P.ANNADURAI, "Impact of Rushing attack on Multicast in Mobile Ad Hoc Network", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.