ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Quantify the Performance of Multicast Mesh Routing Protocol against Collaborative Attack in Wireless Ad-Hoc Networks

Noorunnisa Begum, Hari Prasad Chandika

M.Tech Student, Dept. of C.S.E., SVIET, Andhra Pradesh, India

Associate Professor, Dept. of C.S.E., SVIET, Andhra Pradesh, India

ABSTRACT: Multimedia Communications plays important role in near future Wireless Ad hoc Network. Unicasting and Multicast routing protocols were useful to provide this type of communication. Multicast communication is very useful to transmit data packet to multiple receivers that always gainful in such networks, where bandwidth utilization comes at a premium. This project mainly addresses the mesh based multicast routing protocol and its vulnerability in which mesh based multicast routing protocols that establishes a mesh network and maintains multiple paths between sources to receivers. Due to multiple paths, this protocol is more suitable for frequently changing topological environment and provides more robustness. Moreover, in spite of the routing issue many MANETs applications requires various multicast routing protocols that need to operate correctly even in hostile environment, because the MANETs are more vulnerable to different routing attacks such as wormhole, black hole, rushing attack, man in the middle attack, etc. This paper shows the performance evaluation of mesh based multicast routing protocol against collaborative attack. In order to evaluate this routing protocol, we considered various performance metrics such as end-to-end delay, throughput and packet delivery ratio with varying pause time.

KEYWORDS: Mesh, Multicast, MANETs, Ad hoc network, Collaborative Attack

I. INTRODUCTION

The hardships of researchers in the past decade have brought a profound transformation in our standard of living with the advancement in wireless technology. The wireless network is a promising new technology that will permit users to access information and service everywhere, in spite of their geographic location; Wireless technology is a contemporary substitute to conventional wired networking that relies on cables to connect networkable devices together. Wireless is the word used to illustrate any network where there is no physical wired association between sender and receiver, but moderately radio waves or microwaves to retain communications link the network. Wireless networks offer efficiency, ease, and cost advantages over conventional wired networks. It is necessary to recuperate the network layers in order to provide a flexible and high quality communication system.

Multimedia Communications plays important role in near future Wireless Ad hoc Network. Multicast routing protocols were useful to provide this type of communication. Moreover, it is also very useful to transmit data packet to multiple receivers that always gainful in such networks, where bandwidth utilization comes at a premium. Over the past few years, several multicast routing protocols have been proposed for ad hoc networks with various applications such as battlefield scenarios, policing, search and rescue missions etc. typically involve communication between one commander/supervisor and many troops/ policemen/ volunteers.

This paper mainly addresses the mesh based multicast routing protocol and its vulnerability in which mesh based multicast routing protocols that establishes a mesh network and maintains multiple paths between sources to receivers. Due to multiple paths, this protocol is more suitable for frequently changing topological environment and provides more robustness. Moreover, in spite of the routing issue many MANETs applications requires various multicast routing protocols that need to operate correctly even in hostile environment, because the MANETs are more vulnerable to different routing attacks such as wormhole, black hole, rushing attack, man in the middle attack, etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

This paper also shows the performance evaluation of mesh based multicast routing protocol against collaborative attack. Initially, we modelled multicast routing protocol with varying number of nodes and evaluating its performance with varying number of mobility and traffic patterns. Next, we modeled the collaborative attack against routing protocol to evaluate its performance in hostile environment. In order to evaluate this routing protocol, we considered various performance metrics such as end-to-end delay, throughput and packet delivery ratio with varying pause time.

II. RELATED WORK

This section describes literature review and related work representing the first in-depth into the topic. First, we begin with a wide orbit by reviewing the routing phenomena of such networks proceeded further in the literature applying the radio specific signals as a requisite in detecting PUE attacks like amplitude, frequency and bandwidth. They ever argue that they differ from the previously followed criteria like location, power transmission and the rest, with the view that the values of the radio- specific criteria are the characteristics which can never be changed so easily on the hard-ware post production. The authors have maintained non parametric Bayesian classification while defining the DECLOCK propagated method.

Notwithstanding the presentation of the satisfactory results/outcomes in PUE attacks detection, it has been observed that the DECLOCK can never be adapted easily to the mutations of the behaviour of the attacks, without the need to restructure the same. The Cognitive radio network do not engage the selfish attack that result in the degradation of the performance, where as the secondary users speedup their accessing probability to improve their own utilities. The HELLO attack can be guarded through obviously confirming the bio-directionality of connections before utilizing the connection which is built up by a got message over the same connection. With the assistance of base station which would be a trusted outsider keeping in mind the end goal to encourage the solid foundation of session key among the gatherings which are in the system can likewise offer check to the bi-directionality. This session key allow the imparting nodes in checking the character of one another furthermore gives a connection scrambled between them. It must be watched that the quantity of shared key must be constrained in order to keep any attacker to set up a connection in the middle of every node. On the off chance that if any one node cases to be the neighbour to the over the top number of node, a caution must be raised to identify the attacker. Y.C. Hu et al [19,20], have risen out with a proposition of utilizing packet leashes for distinguishing and shielding against the worm hole attacks.

Here, they show two sorts of packet leashes: fleeting and geographic. The geographic leash has been made utilization of with a specific end goal to guaranteeing the packet beneficiary to a sure separation far from the sender. For the development of geological leash, each and every node must be very much aware of its own area and in this way freely synchronizing the tickers of the considerable number of nodes. In the packets of sending nodes, their own particular area and the season of the packets when it was sent, has been incorporated. The collector node will contrast the information and its own particular area and receipt time. By fancying that the timekeepers of the nodes are fairly approximately synchronized, the beneficiary node can register on upper bound which is on the separation between its own and the sender. It has been watched that the obstructions in the system field should not allow the separation bouncing taking into account area information. Henceforth, the making of worm gaps still done, as the correspondence won't not be allowed between the two nodes that would be generally in the sneak peak of the transmission.

Karlof et al[17]. proposed a technique for the observance of wormhole attack by making utilization of geographic routing protocols for sending the packets in the system. Conventions of such kind develop a topology relying upon the steering activity towards the base station. By the sort of steering technique, are can barely pull in movement towards a wormhole or sinkhole. Nodes that are available locally would be distinguishing the simulated connection for they could without much of a stretch recognize themselves or even between the attackers, is even past the typical radio range.

L.Hou et al. [18], came ahead with a paradigm model to spread a self engendering A1 infection by the method for a cognitive radio structure. By emulating the same the outcome demonstrated that the time that took in contaminating the entire of the cognitive radio system quickly expanded with the possibility of the measure of the system. Also, it demonstrated that the counter infection execution of the static systems is much better when contrasted with the execution of a forceful system in the vicinity of the A1 infection. It even showed that the spread pace of A1 infection increments by the bounteously accessible range asset in the territory. In any case, the pace of the engendering is not influenced by the variability of the spectrum.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Yongle Wu et al, continued more distant in making so as to propel a channel jumping protection procedure utilization of Marko choice procedure approach which is simply taking into account a secondary user utilizing stand out channel. With a specific end goal to copiously use the choice process, the node ought to get some data of the attacker by watching nature. The secondary user at first gauges the helpful parameters which depend on the past perceptions by making utilization of most extreme probability estimation. At this stage the node makes utilization of the Q-learning process that as of now exists as on boulevard for the secondary user for learning and upgrading the safeguard methodology with no recognize of the fundamental Markov model. This entire outline is augmented so as the secondary user makes utilization of the considerable number of channels accessible all the while. In this sort of situation, a randomized designation of force has been utilized as guard system. Determining the Nash harmony for this colonel Blotted amusement offices the minimizing the most pessimistic scenario damage.

III. OVERVIEW TO MULTICAST ROUTING PROTOCOL

In this section, we present the protocol for unified multicasting through announcements (PUMA) in ad-hoc networks, which establishes and maintains a shared mesh for each multicast group, without requiring a unicast routing protocol or the pre assignment of cores to groups. PUMA achieves a high data delivery ratio with very limited control overhead, which is almost constant for a wide range of network conditions. In this protocol, every receiver connects to the elected core along all shortest paths between the receiver and the core. All nodes on the shortest paths between any receiver and the core collectively form the mesh. A sender sends a data packet to the group along any of the shortest paths between the sender and the core. When the data packet reaches a mesh member, it is flooded within the mesh, and nodes maintain a packet ID cache to drop duplicate data packets.

PUMA uses a single control message for all its functions, the multicast announcement. Each multicast announcement specifies a sequence number, the address of the group (group ID), the address of the core (core ID), the distance to the core, a mesh member flag that is set when the sending node belongs to the mesh, and a parent that states the preferred neighbour to reach the core. Successive multicast announcements have a higher sequence number than previous multicast announcements sent by the same core. With the information contained in such announcements, nodes elect cores, determine the routes for sources outside a multicast group to unicast multicast data packets towards the group, notify others about joining or leaving the mesh of a group, and maintain the mesh of the group. A major difference from ROMANT is that the multicast announcement in PUMA alone performs all functions associated with the core announcements and join announcements in ROMANT.

Core Election

PUMA chooses a core per multicast group in each connected component of the network. When a receiver needs to join a multicast group, it first determines whether it has received a multicast announcement for that group. If the node has, it adopts the core specified in the announcement it has received, and it starts transmitting multicast announcements that specify the same core for the group. Otherwise it considers itself the core of the group and starts transmitting multicast announcements periodically to its neighbours stating itself as the core of the group and a 0 distance to itself.

Nodes propagate multicast announcements based on the best multicast announcements they receive from their neighbours. A multicast announcement with higher core ID is considered better than a multicast announcement with a lower core ID. Eventually, each connected component has only one core. If one receiver joins the group before other receivers, then it becomes the core of the group. If several receivers join the group concurrently, then the one with the highest ID becomes the core of the group. A core election is also held if the network is partitioned. The election is held in the partition, which does not have the old core.

IV. MODELLING THE COLLABORATIVE ATTACK AGAINST PUMA

Most of the research has focused on either development of PHY, MAC and routing layer protocols. Moreover, many researches had already proposed many routing protocols and its assaults focusing on cognitive radio ad hoc networks . Within this section, we demonstrate Collaborative Attack which is more devastating that can degrade the performance of the ad hoc networks. This attack will abuse the shortcoming of such networks, due to the requisite transparency of the network performance provided by the routing protocol. Before, we confer the working of this attack, let us compress and give a brief presentation of every assault against protocol for Shared Multicast Announcements

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Collaborative Attack against PUMA Routing Protocol

Let us illustrate with an example how Collaborative attack can be launched in PSMA routing protocol. Here, an attacker node can send MA with its address to another node in the group to impersonate the receiving node, Attacker node can modify the hop count data as it has the shortest path to the destination by sending a MA to the source node, The attacker repeatedly sends MA packet to the source node with its radio range, moreover this malicious node do not forward the MA packets to the source node which was received from its intermediate node, which may leads to the connection Hence, the functionalities of PUMA makes more vulnerable to launch MITM attack, which may degrade the performance of the PUMA routing protocol.

Nodes	Throughput	End-to-end delay	Packet delivery ratio
10	3167.02	5407.50	55.03
20	3140.16	5669.51	54.23
30	3113.3	5931.97	53.43
40	3086.44	6194.43	52.63
50	3059.58	6456.89	51.83

Table 1: Performance metrics for PUMA before attack

Nodes	Throughput	End-to-end delay	Packet delivery ratio
10	1130.90	10004.56	19.54
20	1117.62	10005.45	22.49
30	1104.27	10006.34	25.44
40	1077.41	10007.23	28.39
50	1050.55	10008,12	31.34

Table 2: Performance metrics for PUMA after attack

V. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

To study the feasibility of our theoretical work, we have implemented and evaluated the PSMA, ODMRP and MAODV routing protocols with and without MITM attack using NS-2 parameters as shown in Table 5.1, and conduct a series of experiments to evaluate its effectiveness [4]. The results of this experiment shows that all the three routing protocol affects their performance in the presence of MITM attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

NS-2 Parameters

Propagation Framework	Two Ray Ground
Number of distinct Nodes	10, 25, 50,75,100
Transmission Interval	250m
Simulation Period	150 Seconds
Simulation Vicinity	750m X 750m
Mobility of a Node	Model Random Waypoint
Traffic Nature	FTP/TCP
Payload Size of Data	512 Bytes/Packet
Pause Time of a Node	0-20s
Maximum speed of node	1-20m/s

Table 3: NS-2 Simulation Parameters

To evaluate the performance of these protocols, we considered various performance metrics such as Throughput, Packet delivery fraction, Control overhead, Total overhead with respect to Number of nodes in a group. Packet delivery fraction/ratio: The ratio of total packets delivered to the receiver and number of total packets transmitted by the sender. Throughput: Number of successful packets received from all the sources within simulation t. Control Overhead: (Control Packets transmitted)/(Data Packets Delivered) Total Overhead:(Total Packets Transmitted)/(Data Packets Delivered)

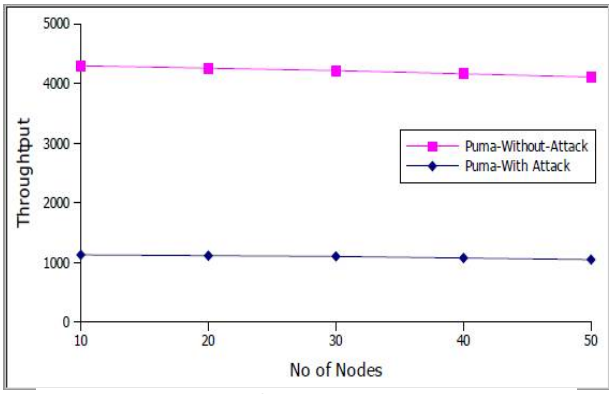

Figure-1 Throughput of PUMA with and Without attack

Figure 1, depicts the throughput Vs varying number of nodes in the group with and without Collaborative Attack. PUMA achieves better throughput as the number of nodes increases in a group. Moreover, it is observed that the PUMA routing protocols perform poorly under Collaborative Attack that is the performance is degraded.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

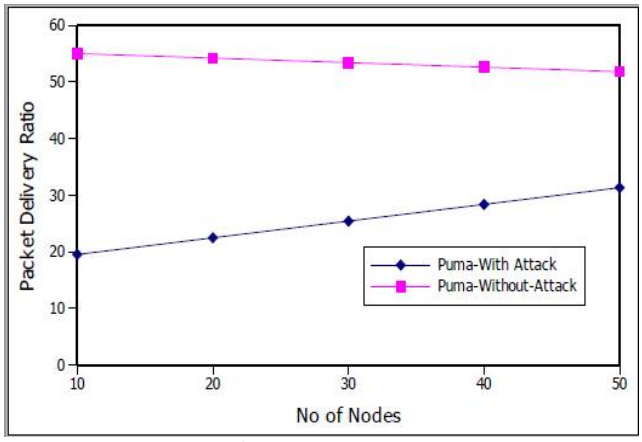

Figure-2 PDF of PUMA with and Without attack

Figure-2 shows the packet delivery fraction with varying number of nodes in a group from 10 to 50 respectively under legitimate and Collaborative Attack situations. The figure shows mesh based multicast routing protocols which gives better results. The figure also shows packet delivery ratio of PUMA under Collaborative Attack. The performances of this routing protocol are degraded slightly compared to legitimate situations.

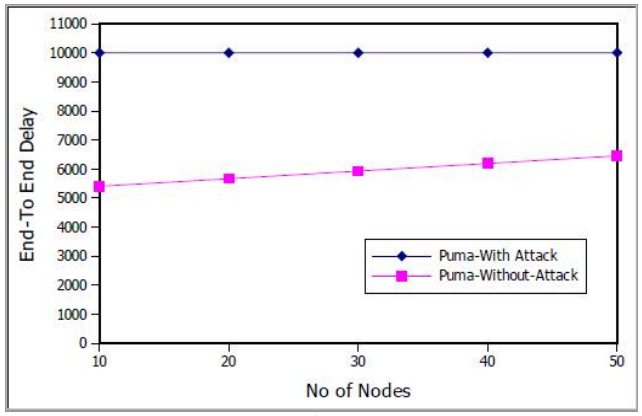

Figure-3 End-To-End -Delay of PUMA with and Without attack

Figure 3 shows the packet end-to-end-delay fraction with varying number of nodes in a group from 10 to 50 respectively under legitimate and Collaborative Attack situations. The figure shows mesh based multicast routing protocols which gives better results. This figure also shows end-to-end-delay of PUMA under Collaborative Attack. The performances of this routing protocol are degraded slightly compared to legitimate situations

VI. CONCLUSION

This paper also shows the performance evaluation of mesh based multicast routing protocol against collaborative attack. Initially, we modelled multicast routing protocol with varying number of nodes and evaluating its performance with varying number of mobility and traffic patterns. Next, we modeled the collaborative attack against routing protocol to evaluate its performance in hostile environment. In order to evaluate this routing protocol, we considered various performance metrics such as end-to-end delay, throughput and packet delivery ratio with varying pause time.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

REFERENCES

1."Multicast Routing Protocols in Mobile Ad Hoc Networks: A Comparative Survey and Taxonomy" by Department of Electrical Engineering, Montreal, Canada.
2. "Exploring Mesh- and Tree Based Multicast Routing Protocols for MANETs" Kumar Viswanath, Katia Obraczka and Gene Tsudik University of California
3. "Analysis of Multicast Routing Protocols: Puma and Odmrp", SSumathy, 1 BeegalaYuvaraj, 2 E Sri Harsha3.
4. Babu, E. Suresh, C. Nagaraju, and MHM Krishna Prasad. "An Implementation and Performance Evaluation Study of AODV, MAODV, RAODV in Mobile Ad hoc Networks." *vol* 4 (2013): 691-695.
5. Babu, E. Suresh, C. Nagaraju, and MHM Krishna Prasad. "Inspired Pseudo Biotic DNA based Cryptographic Mechanism against Adaptive Cryptographic Attacks." *International Journal of Network Security* 18, no. 2 (2016): 291-303.
6. Babu, E. Suresh, C. Nagaraju, and MHM Krishna Prasad. "Light-Weighted DNA-Based Cryptographic Mechanism Against Chosen Cipher Text Attacks." *Advanced Computing and Systems for Security*. Springer India, 2016. 123-144.
7. Babu, E. Suresh, C. Nagaraju, and MHM Krishna Prasad. "Light-Weighted DNA Based Hybrid Cryptographic Mechanism Against Chosen Cipher Text Attacks." *International Journal of Information Processing and Indexed With arXiv, Indian Citation Index-2015, ISSN-0973-821*.
8. Babu, E. Suresh, C. Nagaraju, and MHM Krishna Prasad. "Light-Weighted DNA Based Hybrid Cryptographic Mechanism Against Chosen Cipher Text Attacks." *International Journal of Information Processing and Indexed With arXiv, Indian Citation Index-2015, ISSN-0973-821*.
9. Kumar, S. Ashok, E. Suresh Babu, C. Nagaraju, and A. Peda Gopi. "An Empirical Critique of On-Demand Routing Protocols against Rushing Attack in MANET." *International Journal of Electrical and Computer Engineering* 5, no. 5 (2015).
10. Gopi, A. Peda, E. Suresh Babu, C. Naga Raju, and S. Ashok Kumar. "Designing an Adversarial Model Against Reactive and Proactive Routing Protocols in MANETS: A Comparative Performance Study." *International Journal of Electrical and Computer Engineering* 5, no. 5 (2015).
11. Babu, E. Suresh, C. Nagaraju, and MHM Krishna Prasad. "An Implementation and Performance Evaluation of Passive DoS Attack on AODV Routing Protocol in Mobile Ad hoc Networks." *International Journal of Emerging Trends & Technology in Computer Science* 2, no. 4 (2013): 124-129.
12. Babu, E. Suresh, C. Nagaraju, and MHM Krishna Prasad. "Efficient DNA-Based Cryptographic Mechanism to Defend and Detect Blackhole Attack in MANETs." In *Proceedings of International Conference on ICT for Sustainable Development*, pp. 695-706. Springer Singapore, 2016.
13. Swarna, Mahesh, Syed Umar, and E. Suresh Babu. "A Proposal for Packet Drop Attacks in MANETS." In *Microelectronics, Electromagnetics and Telecommunications*, pp. 377-386. Springer India, 2016.
14. Babu, E. Suresh, C. Nagaraju, and MHM Krishna Prasad. "Analysis of Secure Routing Protocol for Wireless Adhoc Networks Using Efficient DNA Based Cryptographic Mechanism." *Procedia Computer Science* 70 (2015): 341-347.
15. Babu, E. Suresh, C. Nagaraju, and M. H. M. Prasad. "A Secure Routing Protocol against Heterogeneous Attacks in Wireless Adhoc Networks." In *Proceedings of the Sixth International Conference on Computer and Communication Technology 2015*, pp. 339-344. ACM, 2015.
16. C. Karlof and D. Wanger. Secure Routing in Sensor Networks: Attacks and Counter-measures. In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, May, 2003, pp.113-127.
17. L. Hu and D. Evans. Using Directional Antennas to Prevent Wormhole Attacks. In Proceedings of the IEEE Symposium on Network and Distributed System Security (NDSS), 2004.
18.Y.C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. 8th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom'02), ACM Press, 2002
19. Y.C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. IEEE INFOCOM, Mar 2003.

BIOGRAPHY

NOORUNNISA BEGUM studying M.Tech in Dept. of CSE, Sri Vasavi Institute of Engineering and Technology, pedana, Andhrapradesh, India and graduated in B.Tech from the same college Sri Vasavi Institute of Engineering and Technology which is affiliated to JNTUK, in 2013.Her interested area is Network Security

CHANDIKA HARIPRASAD working as Assoc.Professor, in Dept. of CSE, Sri Vasavi Institute of Engineering and Technology, pedana, Andhrapradesh, India and graduated in B.Tech from Vignan's Engineering College which is affiliated to JNTUH, Guntur in 2006. He received Masters Degree in M.Tech. from SIT, JNT University, Hyderabad, in 2009. At present he is doing his research in Network Security. He has published 3 research papers in various National, International journals, conferences proceedings.