Efficient Protocol Prediction Algorithm for MANET Multimedia Transmission Under JF Periodic Dropping Attack

Avita Katal, Mohammad Wazid and R H Goudar

Abstract Mobile ad hoc network is prone to denial of service attack. Jellyfish is a new denial of service attack and is categorized as JF Reorder Attack, JF Periodic Dropping Attack, JF Delay Variance Attack. In JF Periodic Dropping Attack, intruder node intrudes into forwarding group and starts dropping packets periodically. Due to JF Periodic Dropping attack, the delay in the network increases and throughput decreases. In this paper a comparative performance analysis of three reactive routing protocols i.e. AODV, DSR and TORA used in mobile ad hoc network under JF Periodic Dropping attack is done. This work is specially done for multimedia transmission i.e. video and voice. If we have a mobile ad hoc network in which probability of occurrence of JF Periodic Dropping attack is high and also if it requires time efficient network multimedia service for information exchange then TORA protocol is to be chosen. If it requires high multimedia throughput and consistent service in the network then AODV protocol is recommended. An algorithm has been proposed depending upon the analysis done particularly for multimedia transmission in MANET which will help in choosing the best suited protocol for the required network parameters under JF Periodic Dropping attack.

Keywords JF periodic dropping attack · Multimedia transmission · AODV · DSR · TORA

A. Katal (✉) · M. Wazid · R. H. Goudar
Department of CSE, Graphic Era University, Dehradun, India
e-mail: avita207@gmail.com

M. Wazid
e-mail: wazidkec2005@gmail.com

R. H. Goudar
e-mail: rhgoudar@gmail.com

B. V. Babu et al. (eds.), *Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28–30, 2012*, Advances in Intelligent Systems and Computing 236, DOI: 10.1007/978-81-322-1602-5_45,

1 Introduction

An intruder can easily access mobile ad hoc network because of weak defense mechanism and high mobility of nodes. Multimedia transmission includes streaming of multimedia to an end user by the provider. It mainly includes voice and video transmission. MANET assailable to JF Periodic Dropping attack increases the end to end delay between selected packets in a flow with any lost packets being ignored. This is called Jitter which increases under the above mentioned attack leading to degradation in the quality of the media being transmitted. In this paper the impact of presence of JF Periodic Dropping attack on the performance of network transmitting multimedia is analyzed. Comparative analysis of the three routing protocols i.e. AODV, DSR and TORA used for the transmission of multimedia for various network parameters is done. Section 2 includes the literature review about different kinds of work done by various authors in area related to JellyFish attacks. The novelty of the proposed idea is discussed in Sect. 3. In Sect. 4 a brief introduction to JellyFish attack is given. The methodology and experiment design of this work is discussed in Sect. 5. Section 6 contains performance parameters and results. Section 7 includes the algorithm for protocol prediction designed on the basis of results obtained followed by conclusion, future work and application of the work done in Sect. 8.

2 Literature Review

Paper [1] discusses about techniques for resilience of denial of service attacks on a mobile ad hoc network focusing on JellyFish attacks. The throughput of network under JellyFish attacks introduced here is calculated. Techniques to protect MANET i.e. flow-based route access control (FRAC), Multi-Path Routing Source-Initiated Flow Routing, Sequence Numbers etc are discussed. In [2] authors calculate the performance of MANET under black hole attack using AODV routing protocol with HTTP traffic load. In [4] authors explain various attacks on a mobile ad hoc network corresponding to different MANET layers and they also discuss some available attack detection techniques. They give a brief idea about JellyFish attack. In [5] the performance of different routing protocols for multimedia data transmission over vehicular ad hoc networks is done. The focus was put on the performance evaluation metrics that were used in simulations. Three popular routing protocols were selected for the evaluation: two reactive (AODV, DSR) and one proactive (OLSR). In [6] authors develop an algorithm that detects the Jellyfish attack at a single node and that can be effectively deployed at all other nodes. A novel metric depending on reorder density is proposed and comparison table is given which shows the effectiveness of novel metric which helps protocol designers to develop the counter strategies for JF attack. The main objective of [7] is to analyze and compare the performance of Preemptive DSR and temporarily ordered routing algorithm (TORA). It discusses the effect of variation in number of nodes and average speed on protocol performance.

It concludes that PDSR outperforms TORA in terms of the number of MANET control packets used to maintain or erase routes. TORA is a better choice than PDSR for fast moving highly connected set of nodes. In [8] an attempt has been made to compare the performance of two prominent on demand reactive routing protocols for MANETs: ad hoc on demand distance vector (AODV), dynamic source routing (DSR) protocols. It concludes that if the MANET has to be setup for a small amount of time then AODV should be preferred due to low initial packet loss. If we have to use the MANET for a longer duration then both the protocols can be used, because after sometime both the protocols may have same ratio of packet delivering. But AODV have very good packet receiving ratio in comparison to DSR. In [10] the performance of DSR and TORA routing protocols is calculated using the OPNET simulator. It concludes that delay experienced with mobile nodes employing DSR routing is higher than that of fixed nodes. Delay experienced with fixed nodes employing TORA routing is higher than that of mobile nodes. In [12] authors discuss the most common types of attacks on MANET, namely Rushing attack, Blackhole attack, Neighbor attack and JellyFish attack. They simulate these attacks and calculate parameters such as Average end-to-end delay, Average throughput etc. In Paper [13] JellyFish and Black hole attacks are discussed. Authors calculate the impact of JF on the system performance i.e. Throughput etc. They introduce three factors: mobility, node density and system size and calculate the effect of these factors on fairness to receive packets under the presence of various number of JF attackers. They observe that the effect of mobility is more under the absence of JF attackers and fairness reduces when we increase mobility.

3 Problem Definition and Novelty

Previously many authors have analyzed the performance of various MANET protocols for multimedia transmission. In this paper the performance analysis of the most popular reactive routing protocols in the multimedia transmission under JF Periodic Dropping attack is done followed by an algorithm used for selecting the best suited routing protocol for transmitting multimedia with the desire network parameters.

4 JellyFish Attack

JellyFish attack is related to transport layer of MANET stack. The JF attacker disrupts the TCP connection which is established for communication. JellyFish (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. JF attacker disrupts the whole functionality of TCP, so performance of real time applications become worse. JF attack is further divided into

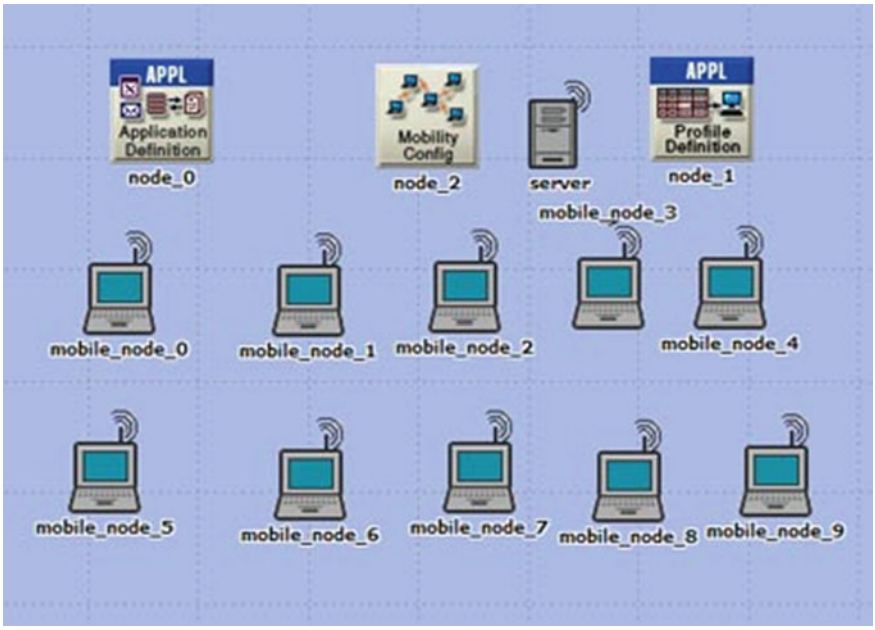

Fig. 1 MANET under normal flow

three categories- JF Reorder Attack, JF Periodic Dropping Attack, JF Delay Variance Attack.

4.1 JF Periodic Dropping Attack

In this attack the JF attackers drop all packets for a short duration of time. Thus JF nodes seem passive in nature and do not generate traffic themselves. JF nodes drop packets for only a small fraction of time due to dropping of packets the performance becomes worse [1].

5 Methodology and Experiment Design

For experimental purpose we simulate a mobile ad hoc network under JF Periodic Dropping attack for three reactive routing protocols i.e. AODV, DSR and TORA using Opnet modeler. We are using the following two simulation scenarios in this paper:

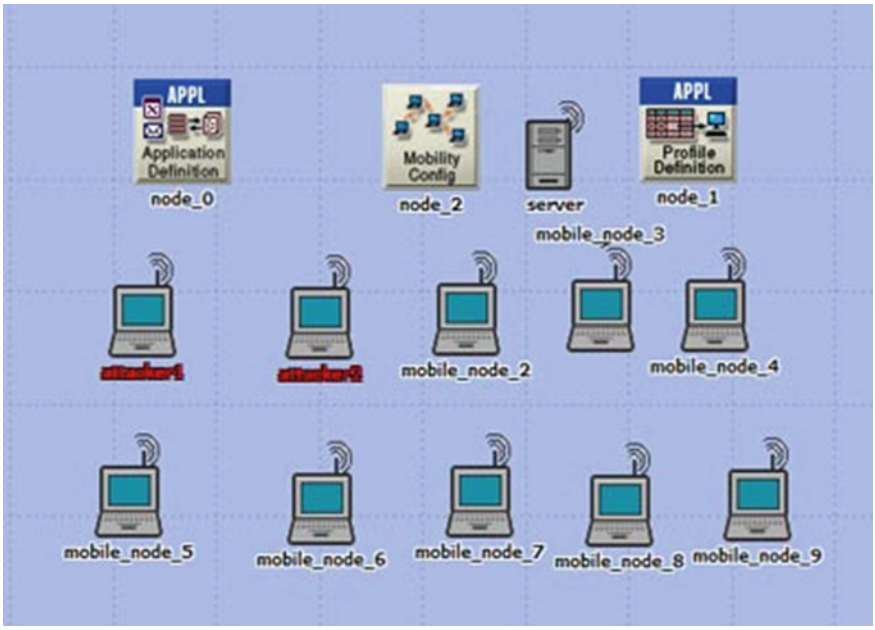

Fig. 2 MANET under jellyfish attack

In Fig. 1 we use 10 mobile nodes and build a scenario without any JF attacker showing a normal flow of traffic. In Fig. 2 we use 10 mobile nodes and build a scenario with two JF Periodic Dropping attackers. JF attackers are shown in red label i.e. attacker 1 and attacker 2. All scenarios are simulated using AODV, DSR and TORA protocols.

The experimental design setup is used to examine the performance of three reactive routing protocols under JF Periodic Dropping attack in MANET transmitting multimedia data.

5.1 Experiment Design Parameters

5.1.1 Common Parameters

Implementations of JF Periodic Dropping Attack

The normal packet forwarding rate is 100,000 packets per second and simulation time is ten minutes. To simulate JF Periodic Dropping attack the time of periodic dropping is taken to five minutes. During other five minutes there is normal flow. Given two scenarios are simulated under routing protocols i.e. AODV, DSR and TORA (Table 1).

Table 1 Common parameters used in simulation

Parameter	Value
Platform	Windows XP SP2
Simulator	Opnet modeler 14.5
Area	500 × 500 m (Fix)
Network size	10 nodes
Mobility model	20 m/s (Fix)
Traffic type	Video and Voice both
Simulation time	10 min
Address mode	Only IPv4
Ad Hoc routing protocol	AODV, DSR, TORA
AODV, DSR, TORA, TCP parameters	Default
JellyFish attackers	Zero attacker for normal flow (Scenario 1)
	Two attackers (Scenario 2)
Attacking scenario	For 5 min, normal flow
	For 5 min, flow under JF packet dropping
Packet size (bits)	Exponential (1024)

Table 2 End-to-end delay and throughput

Parameters	End-to-end delay (s)		Throughput (bps)	
Protocol	Normal flow	Under attack	Normal flow	Under attack
AODV	6.72	8.47	51573.91	41517.39
DSR	7.74	10.32	25832.07	19263.31
TORA	6.87	8.47	21714.92	16903.32

5.2 Results

In simulation we take following statistics of the network: End-to-end Delay (msec), Throughput (bps).

Figure 3 shows end-to-end delay with normal flow (zero attackers) and also in the presence of JF attackers for all given three protocols. Figure 4 shows throughput

Fig. 3 End-to-end delay

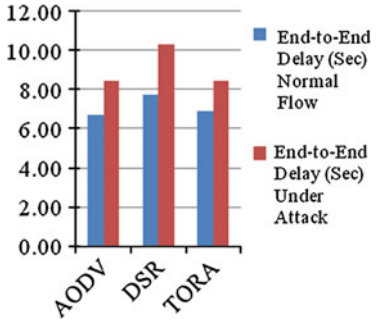

Fig. 4 Throughput (bps)

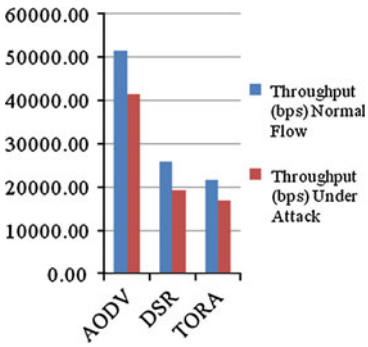

Fig. 5 Impact of JF periodic dropping attack

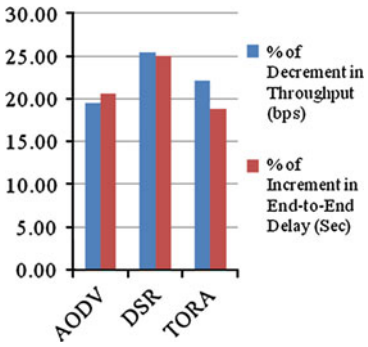

Table 3 Impact of JF periodic dropping attack on end-to-end delay and throughput

Protocol	% of Decrement in throughput (bps)	% of Increment in end-to-end delay (Sec)
AODV	19.50	20.66
DSR	25.43	25.00
TORA	22.16	18.89

(bps) with normal flow (zero attackers) and also in the presence of JF attackers for all given three protocols.

Figure 5 shows impact of JF Periodic Dropping attack on end-to-end delay and throughput for all given three protocols.

6 Protocol Prediction Algorithm

enum protocol set => {AODV,TORA,DSR}
enum service set => {Throughput Efficient, In Time}
if service = Throughput Efficient then

```
    select_protocol = AODV
otherwise if service = In Time then
    select_protocol = TORA
otherwise
    select_protocol = DSR
```

Complexity Analysis:
The complexity of protocol prediction algorithm comes to be $\ominus$ (1) in combination with the complexity of AODV, TORA or DSR. We can say the complexity of the above algorithm comes in the order of the complexity of the AODV, TORA or DSR.

The above algorithm designed is basically used for choosing the appropriate reactive routing protocol out of the set of three protocols i.e. AODV, DSR and TORA for efficient multimedia transmission depending upon the network parameter requirements that is throughput efficiency and in time delivery.

7 Key Findings

Here, we try to evaluate the performance of three reactive protocols i.e. AODV, DSR and TORA which are implemented in mobile ad hoc network under the presence of JF Periodic Dropping attack for multimedia transmission. Some of the observations are as:

- The performance of DSR is worst for both the network parameters i.e. throughput and delay in multimedia transmission (as shown in Table 2).
- In multimedia transmission a throughput efficient service is provided by AODV protocol as compared to DSR and TORA. The % of decrement in throughput for AODV is 19.50 as compared to DSR and TORA which are having a decrement of 25.43 and 22.16 respectively (as shown in Table 3).
- Multimedia time demanding service must use TORA protocol as TORA proves to be more efficient under JF Periodic Dropping attack with a % increment of end-to-end delay of 18.89 as compared to AODV and DSR which are having 20.66 and 25.00 respectively (as shown in Table 3).

8 Conclusion

If we have a mobile ad hoc network in which probability of occurrence of JF Periodic Dropping attack is high and we want a good time efficient network multimedia service then we have to choose TORA protocol whereas good throughput multimedia

service should make use of AODV protocol (as shown in Table 3). Depending upon these results the protocol prediction algorithm is proposed which efficiently chooses the required protocol for multimedia transmission.

Here 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.

There are certain applications which can bear the time inefficiency but require high throughput service as in case of virtual classrooms where the student can attend lectures even when they are not sitting in the campus class whereas in case of Warfield the time efficiency would be important as compared to throughput. Depending upon these different requirements for different scenarios we recommend AODV for virtual classrooms and TORA for Warfield applications.

References

1. Begum, S. A., Mohan, L., Ranjitha, B.: Techniques for resilience of denial of service attacks in mobile ad hoc networks. In: Proceedings published by International Journal of Electronics Communication and Computer Engineering, Vol. 3(1), NCRTCST, ISSN 2249–071X National Conference on Research Trends in Computer Science and Technology (2012)
2. Barkhodia, E., Singh, P., Walia, G. K.: Performance analysis of AODV using HTTP traffic under Black Hole Attack in MANET. Comput. Sci. Eng. Int. J. (CSEIJ). **2**(3), (2012)
3. Jan, V. M., Welch, I., Seah, W. K. G: Security threats and solutions in MANETs: A case study using AODV and SAODV. Elsevier J. Netw. Comput. Appl. **35**, 1249–1259 (2012)
4. Wazid, M., Singh, R. K., Goudar, R. H.: A survey of attacks happened at different layers of mobile ad-hoc network and some available detection techniques. In: Proceedings published by International Journal of Computer Applications (IJCA) International Conference on Computer Communication and Networks CSI- COMNET, Hawaii, December (2011)
5. Adam, G., Kapoulas, V., Bouras, C., Kioumourtzis, G., Gkamas, A., Tavoularis. N.: Performance evaluation of routing protocols for multimedia transmission over mobile ad hoc networks. In: IEEE International Conference on Wireless and Mobile Networking Conference (WMNC), (2011)
6. Jayasingh, B. B., Swathi, B.: A novel metric for detection of jellyfish reorder attack on ad hoc network. BVICAM'S Int. J. Inf. Technol. (BIJIT) **2**(1), ISSN 0973–5658 (2010)
7. Ramesh, V., Subbaiah, P., Koteswar Rao, N., Subhashini, N., Narayana.D.: Performance comparison and analysis of preemptive-DSR and TORA. Int. J. Ad hoc, Sens. and Ubiquitous Comput. (IJASUC) **1**(4) (2010)
8. Thakare, A. N., Joshi, M. Y.: Performance analysis of AODV & DSR routing protocol in mobile ad hoc networks. IJCA Special Issue on Mobile Ad-hoc Networks MANETs (2010)
9. Cai, J., Yi, P., Tian, Y., Zhou, Y., Liu, N.: The simulation and comparison of routing attacks on DSR protocol. In: IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCom), Beijing, September (2009)
10. Amer, S. H., Hamilton, J. A.: DSR and TORA in fixed and mobile wireless networks. In: Proceedings of ACM-SE, ACM, Auburn, March (2008)
11. Alshanyour, A. M., Baroudi, U.: Bypass AODV: improving performance of ad hoc on- demand distance vector (AODV) routing protocol in wireless ad hoc networks. In: Proceedings of ACM Ambi-sys, ACM Digital Library, Quebec city, 11–14 February (2008)

12. Nguyen, H. L., Nguyen, U. T.: A study of different types of attacks on multicast in mobile ad hoc networks. Elsevier J. Ad Hoc Netw. **6**, 32–46 (2008)
13. Aad, I., Hubaux, J.-P., Knightly, E. W.: Denial of service resilience in ad hoc networks. In: Proceedings of ACM MobiCom, Philadelphia, Sept. 26–Oct.1 (2004)