Performance evaluation of routing protocols under security attacks in mobile ad hoc networks

Kashif Hussain Memon[†], Muhammad Ali Qureshi[†], Sufyan Memon[††], Mohsin Shaikh[†††], Ramesh Kumar[††††]

[†]University College of Engineering & Technology, The Islamia University of Bahawalpur, Pakistan
[††]Department of Mechanical, Aerospace and Nuclear Engineering, UNIST, Ulsan, South Korea
[†††]Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah, Pakistan
[††††]Department of Electronic Engineering, Dawood University of Engineering & Technology, Karachi, Pakistan

Summary
Security in the wireless ad hoc network is being considered as a great issue due to the absence of central authority and a priori trustworthy relationship. Moreover, the wireless links are also prone to eavesdropping, replay, and spoofing attacks. The existing security features developed for the wired networks are not well suited for the wireless ad hoc networks. A lot of problems may occur in the mobile ad hoc network only due to the security threats in routing protocols. This work mainly aims to perform the analysis of security features in Ad hoc on demand Distance Vector (AODV) and Destination Sequence Distance Vector (DSDV) routing protocols. The effects of fake distance vector (FDV) and fake destination sequence (FDS) security attacks on AODV and DSDV protocols are analyzed through the simulation. Three quantitative measures i.e., delivery ratio, communication overhead of the FDV and FDS attacks, and the spreading of fake routes are used for performance evaluation. We conclude with the justification of the results. This work will help in designing new robust routing protocols against various security attacks.

Key words:
Ad hoc network security; Routing protocols; Ad hoc on-demand distance Vector (AODV); Destination Sequence Distance Vector (DSDV);

1. Introduction

Mobile Ad hoc networks (MANETs) are the class of wireless networks without any fixed infrastructure like mobile switching centers (MSC) or base stations (BS) [1,2]. Every user in this network work as a router to forward information to other users in the network (see Fig. 1). The choice of user to forward data relates to the network topology and dynamic network connectivity. The major applications of MANETS are rescue operations, meetings and conventions for rapid information sharing, and data acquisition in a hostile environment. Despite vast advantages of wireless ad hoc network, some challenging areas need proper attention.

(i) Network topology changes dynamically in MANETs [3].

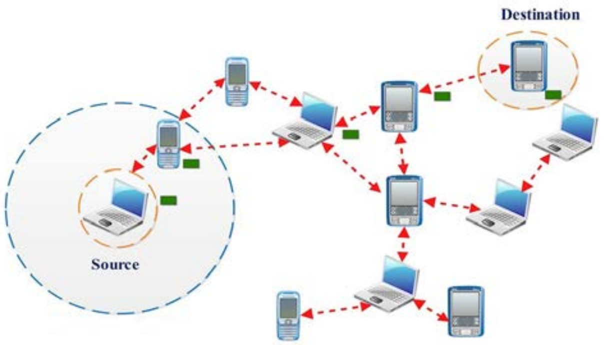

Fig. 1 An example of mobile ad hoc network

(ii) Mobile nodes of different types and weight transmit and receive at different power level, which create asymmetric links.
(iii) Nodes in MANETs disconnect frequently.
(iv) Security in ad hoc network is a major design challenge [4].

Different types of routing protocols are being used in MANETs. Commonly used one are Ad hoc On demand Distance Vector (AODV) and Destination Sequence Distance Vector (DSDV) protocols. These protocols are prone to the security attacks. In this work, we study the effects of various security attacks on AODV and DSDV and the performance of these protocols is evaluated using some quantitative measures.

The rest of the paper is organized as follows. In Section 2 and 3, we discuss briefly the routing protocols and security attacks respectively. We discuss the details of simulation experiments and results in Section 4 and 5 respectively. Finally, the paper is concluded in Section 6.

2. Routing Protocols in MANETs

Routing in MANETs is considered as an important aspect and in this regard, numerous routing protocols have been

Manuscript received December 5, 2017
Manuscript revised December 20, 2017

proposed in the literature. We can broadly categorize these protocols into proactive and reactive routing protocols [5-8].

2.1 Proactive routing strategy

In proactive routing in MANETs, every node keeps latest routing information about other nodes in the network. The establishment and maintenance of the routes are done using a combination of periodic and event-triggered routing updates. Periodic updates involve the exchange of routing information with other nodes at regular time intervals, irrespective of the mobility and traffic properties of the network. Whereas, event-triggered updates occur on the appearance of some event like addition or removal of links. The Destination Sequence Distance Vector (DSDV) is one of the examples of proactive routing protocols [7, 9]. The DSDV routing protocol is an extension of classical Bellman ford routing algorithm. In DSDV, routes are created using routing tables from each node. In DSDV protocol, each node broadcasts the routing table update packets throughout the entire network at regular time intervals without considering the load in the network, to keep inform routing details to other nodes. Loop-free routing is considered as the major benefit of DSDV. The proactive property of DSDV also creates problems for the malicious hosts to carry on attacks. However, communication overhead is considered as the major limitation as for the size of the routing table and the bandwidth required to transmit update packets increases with the number of nodes in the network.

2.2 Reactive routing strategy

Reactive routing protocols are used to maintain routing information when it is required. It reduces the overhead of updating routing information in routing tables for all time intervals. However, the major limitation of reactive routing is the route acquisition latency means that whenever a source node needs a route, it takes time to find the route. The Ad hoc On-demand Distance Vector (AODV) is an example of reactive routing protocol [7, 10]. The nodes create routes on-demand basis and maintain only the required route information and resulting in reduced routing table size and reduce network bandwidth. It is also scalable to a large number of nodes. However, the AODV usually suffers from large delays while routing initial packets due to the unavailability of a route.

3. Security Attacks

Security is one of the big issues in both wired and wireless network [11]. In MANETs, the communication is done in free space and is prone to various security threats such as replay, spoofing, and eavesdropping. The security attacks are either passive or active attacks. In passive attacks, the attacker listens to the traffic of other users to gain knowledge of message contents. Examples of active attacks are 1) eavesdropping, where attackers analyze the transmission and obtain the contents of messages. 2) Flooding, where the network is flooded with messages in short time and results in wastage of resources. 3) Dropping, where a packet is dropped without any reason to destroy the routing. 4) Cooperation, non-cooperative behavior in MANETs results in Denial of Service (DoS) attacks. In this work, we did not consider the effects of passive attacks on routing protocols.

Active attacks inject erroneous routing information and create congestion and completely traffic blocking in the network. In contrast to the passive attacks, the attacker in active attacks not only monitors the traffic but also attempts to disrupt the network service by inserting false information. Examples of active attacks are 1) Impersonation, where an attacker portrays as a trustworthy user and involves in the redirection of routing messages without authentication. 2) Delay, where messages are delayed without deliberately to destroy network availability and access control mechanism. 3) Replay, where messages are stored and resend to destroy the transmission integrity. In this work, we observe the effects of two active attacks i.e., Fake Distance Vector (FDV) attack and Fake Destination Sequence (FDS) attack on both AODV and DSDV protocols.

The FDV attacks occur due to dynamic change in the network topology in MANETS. The attacker node argues for updating routing packets even without availability of free routes. The data packets may lost in case of route provided by the attacker node. Whereas, in FDS attacks, the originality of routing information is recognized by using destination sequence for both DSDV and AODV routing protocols. In MANETs, the route with largest sequence number is always preferred when more routes are available. The attacker exploits this option and sets a large fake destination sequence number to the routing packets, to make its route preferable for conducting attacks on the user data. The attacker node distributes this information to other nodes as well to make its attack more powerful.

4. Simulation Experiments

The paper aims to observe the performance of two different categories of routing protocols. In this regard, we observe the effects of FDV and FDS security attacks on both proactive (i.e., AODV) and reactive (i.e., DSDV) routing protocols. The simulation is carried out in three stages i.e., pre-simulation, execution, and post-simulation stages. The pre-simulation stage involves the creation of both scenario and communicating files to show the moving

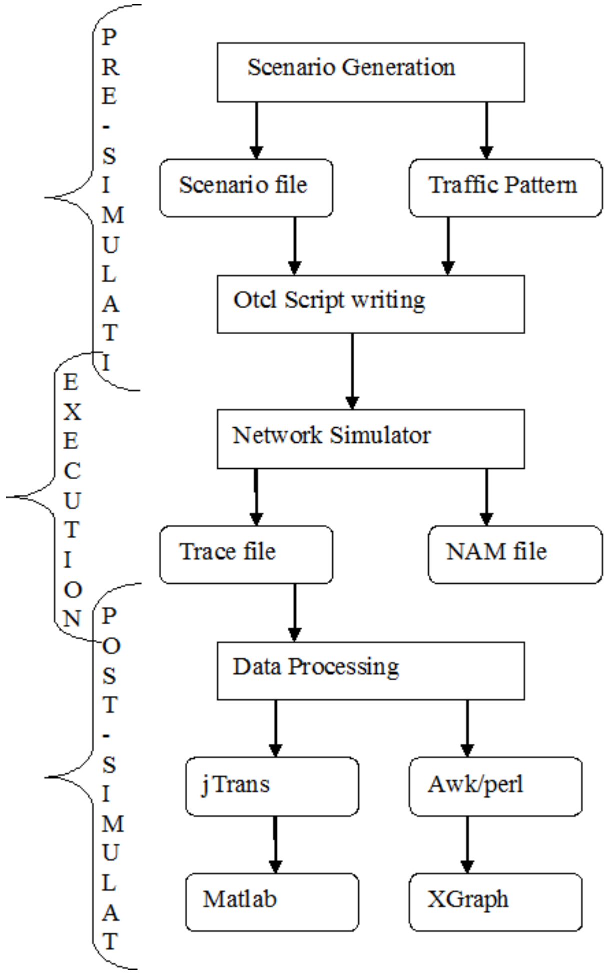

Fig. 2 Flow chart of the proposed methodology

nodes and traffic patterns in the network. It also involves the writing of OTcl script for simulating routing protocols. The execution stage is responsible for creating a trace file (a rough form of data) from the OTcl script. The trace file keeps the information related to the number of data/control packets received, sent, forwarded, and missed. Finally, in the post-simulation stage, the useful information is extracted from the trace file. The results are plotted using XGraph application by interpreting the trace file using Perl and Awk scripts. Alternatively, the trace file is interpreted using jtrans application and results are plotted in Matlab. Fig. 2 shows the flowchart of the simulation steps used in the proposed methodology.

4.1 Simulation Setup

The simulation is performed on an Intel machine with 2.0 GHz processor and Linux Fedora 8 operating system. The script is written in C++ and OTcl programming languages and simulated using network simulator 2 (NS-2) [12]. The parameters used for the simulation are listed in Table1.

Table 1: Summary of parameters used for the simulation

Parameter	**Values**
Simulator	ns-2
Protocols evaluated	AODV, DSDV
Attacks examined	False distance vector, False destination sequence
Simulation time	1000 seconds
Simulation area	1000 x 1000 m
Number of mobile hosts	30
Transmission range	250 m
Movement model	Random waypoint
Maximum speed	5-20 m/s
Traffic type	CBR (UDP)
Payload size	512 bytes
Packet rate	2 packets/second
Number of malicious host	1
Host pause time	10 seconds

For simulation purposes, we assume that all the connections have different sources and node 5 and 29 behave as attacker and destination nodes respectively. There exist twenty-eight maximum connections excluding the attacker node (node 5) and destination node (node 29) from different sources to reach to the destination node.

The attacker node in AODV protocol generates Route Reply (RREP) messages on receiving of Route Request (RREQ) messages from other nodes. Whereas, the attacker node sends false routing messages to the destination node in DSDV protocol. In addition to sending fake route messages, the attacker also involves in dropping of messages. For simulation purposes, we assume that destination is the same for all the links. We also assume that host is not moving very fast, because rapid changes in routes may create ambiguity in the results.

¥subsection{Performance metrics}
The performance of routing protocols against security attacks is evaluated using three metrics i.e., packet delivery ratio, communication overhead, and nodes affected by false routes.

(i) Packet delivery ratio is calculated between the affected packets and total number of packets transmitted to determine the attack intensity.
(ii) Fake routing packets transmitted by the attacker are measured to observe the communication overhead of various attacks.
(iii) Number of normal nodes deceived by the fake routes are determined to disseminate fake routes.

5. Results and Discussions

In this work, we simulate the effect of attacker for the three measures discussed before against different number of connections. The points in the graphs are the average of the values taken from ten different scenarios.

5.1 Results for packet delivery ratio:

The packet delivery ratio is evaluated against a number of connections under three scenarios for security attacks i.e. FDV, FDS, and no attack and results are plotted as Fig. 3. From the plots, we observe that in case of not attack scenario, the packet delivery ration is in the range 92¥% - 96¥% for AODV routing protocol and gradually decreases with increase in the number of connections whereas, packet delivery ratio remains almost constant as the number of connection increases for DSDV protocol. Secondly, in case of FDS attacks encountered by malicious node 5, a significant decrease in packet delivery ratio is observed compared to the FDV attacks for both protocols. The reason is that new routes are always preferred against short routes by DSDV and AODV protocols. Moreover, the impact of FDS attacks on the packet delivery ratios is related to the behavior of attacker itself. In AODV, the attacker node adds a wrong sequence number to that of received routing update message or sends RREP message with the fake sequence number. Whereas in DSDV protocol, the false sequence number is spread to the network instantly. Due to this, the number of nodes affected is higher in DSDV protocol compared to that in AODV protocol. Additionally, in case of FDS attack on AODV protocol, the packet delivery ratio slightly increases as the number of connections increase. The reason is the attacker only adds a constant value to the sequence number in AODV protocol. It will result in a fast increase of actual sequence number with an increase in the number of connections.

5.2 Results for number of affected nodes:

The plots for normal nodes affected by fake routes against the number of connections are shown in Fig. 4. From the results, it is clear that in case of DSDV protocol, the number of affected nodes is almost same with the number of connections due to the dynamic proactive property. In case of FDS attack, almost all the nodes are deceived, whereas around less than half of the nodes are deceived in case of FDV attack. It is clearly demonstrated that a large number of nodes are affected in case of FDS attack since both protocols prefer the routes with a large sequence number. We also observe that in case of AODV protocol, less nodes are affected compared to the DSDV protocol.

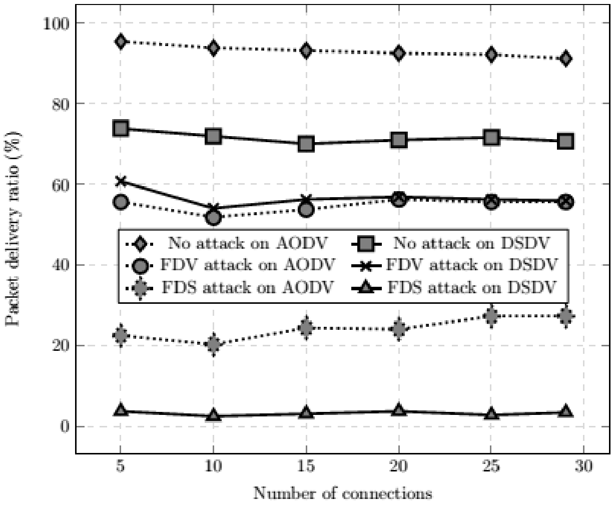

Fig. 3 Packet delivery ratio versus number of connections

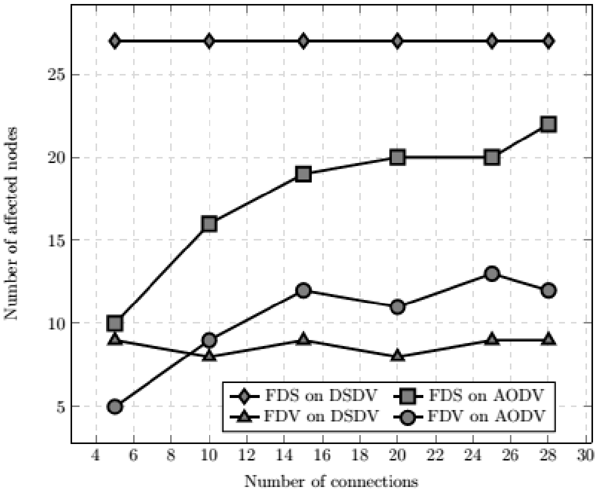

Fig. 4 Number of affected nodes versus number of connections

5.3 Results for number of false packet routes:

To observe the communication overhead of the two attacks, we determine the number of fake route packets against the number of connections and show the results in Fig. 5. We observe that for DSDV routing protocol, number of false route update packets is almost constant and impact of the two attacks is indistinguishable. Whereas, in case of AODV protocol, the number of false packet routes is almost directly proportional to the number of connections. It is also observed that both attacks result in same communication overhead, however, the impact of FDS attack is slightly greater than the FDV attack. This is due to the reason that the attacker causes disturbances in update process of true sequence number by establishing fake sequence.

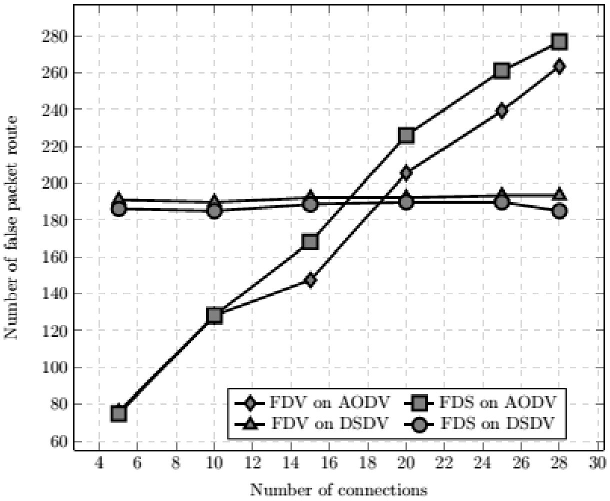

Fig. 5 Number of false packets versus number of connections

6. Conclusion

Security is considered as a big concern in both wired and wireless network. It is also very important to deal with the security aspects of ad hoc network. In this work, the impact of two security attacks (FDV and FDS) on both proactive (DSDV) and reactive (AODV) routing protocols were analyzed. We demonstrated that AODV performs well in terms of less communication overhead. The FDS attack is more critical compared to the FDV one because; both routing protocols prefer the short routes. We observed that packet delivery ration is very less in case of FDS attacks for both protocols. Similarly, the nodes affected due to the FDV attack are less than 50% for both protocols. Moreover, the communication overhead is also almost constant for different number of connections in DSDV protocol.

References

[1]. C. E. Perkins et al., Ad hoc networking. Addison-wesley Reading, 2001, vol. 1.

[2]. J. Loo, J. L. Mauri, and J. H. Ortiz, Mobile ad hoc networks: current status and future trends. CRC Press, 2016.

[3]. N. Nikaein and C. Bonnet, “Topology management for improving routing and network performances in mobile ad hoc networks,” Mobile Networks and Applications, vol. 9, no. 6, pp. 583–594, 2004.

[4]. A.-S. K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press, 2016.

[5]. F. Lee, “Routing in mobile ad hoc networks,” in Mobile Ad-Hoc Networks: Protocol Design. InTech, jan 2011. [Online]. Available: https://doi.org/10.5772%2F13155

[6]. M. K. Marina and S. R. Das, “Routing in mobile ad hoc networks,” Ad Hoc Networks, pp. 63–90, 2005.

[7]. E. M. Royer and C.-K. Toh, “A review of current routing protocols for ad hoc mobile wireless networks,” IEEE personal communications, vol. 6, no. 2, pp. 46–55, 1999.

[8]. M. Abolhasan, T. Wysocki, and E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks,” Ad hoc networks, vol. 2, no. 1, pp. 1–22, 2004

[9]. C. E. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers,” in ACM SIGCOMM computer communication review, vol. 24, no. 4. ACM, 1994, pp. 234–244.

[10]. C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc on-demand distance vector (AODV) routing,” Tech. Rep., jul 2003.

[11]. P. Papadimitratos and Z. J. Haas, “Secure routing for mobile ad hoc networks,” in the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), Jan 2002, pp. 193–204.

[12]. T. Issariyakul and E. Hossain, Introduction to network simulator NS2. Springer Science & Business Media, 2011.

Kashif Hussain Memon
He is currently working as Assistant Professor in Computer Systems Engineering Department, University College of Engineering & Technology, The Islamia University of Bahawalpur. He received the B.E. degree in software engineering, M.E. degree in Communication System and Networks from Mehran University of Engineering & Technology Jamshoro, Hyderabad, Pakistan in 2006 and 2008 respectively. He received his Ph.D. degree from Hanyang University ERICA Campus, South Korea. His research interests include pattern recognition, computer vision, application of fuzzy set theory, and clustering techniques with applications to image segmentation and content-based image retrieval.

Muhammad Ali Qureshi
He is currently working as Assistant Professor in Telecommunication Engineering Department, University College of Engineering & Technology, The Islamia University of Bahawalpur. He received his B.Sc. degree in electrical engineering from UET Lahore in 2000 and M.Sc. in telecommunication engineering from NWFP-UET Peshawar in 2008. He completed his Ph.D. in Electrical Engineering from KFUPM, Saudi Arabia in January 2017 His research interests include image & video processing, image compression, image forensics, and image quality assessment. He has published 18 refereed international journals and conference papers. He is the reviewer of Signal Processing: Image Communication, Multimedia Tools and Applications, and IEEE Sensors journals.

Sufyan Memon received the B.E. degree in electronics engineering, M.E. degree in Electronic Systems Engineering from Mehran University of Engineering & Technology Jamshoro, Hyderabad, Pakistan in 2008 and 2012 respectively. He received his Ph.D. degree in Electronic Systems Engineering from Hanyang University ERICA Campus, South Korea. He is currently post-doc student at UNIST, Ulsan, South Korea. His research interests include pattern recognition, Target tracking.

Mohsin Shaikh received the B.E. degree in software engineering from Mehran University of Engineering & Technology Jamshoro, Hyderabad, Pakistan in 2006. M.S. degree in Computer Science & Engineering from Hanyang University ERICA Campus, South Korea in 2010. Ph.D. degree in Computer Science & Engineering from Chung-Ang University, Seoul, Korea, 2017. His research interests include software engineering.

Ramesh Kumar received the B.E. degree in computer systems engineering from Mehran University of Engineering & Technology Jamshoro, Hyderabad, Pakistan in 2006. He received his M.S. and Ph.D. degrees in Electronic, Electrical, Control and Instrumentation Engineering, and Electronics and Computer Engineering from Hanyang University South Korea in 2010 and 2017 respectively. His research interests include commutation systems, MIMO technology, smart grid networks, and delay tolerant network.