Secure and Efficient Routing Mechanism in Mobile Ad-Hoc Networks

Masroor Ali[1], Zahid Ullah[2], Meharban Khan[3], Abdul Hafeez[4]
Department of Electrical Engineering, CECOS University of IT and Emerging Sciences, Peshawar, Pakistan[(1,2,3)]
Department of Computer Science and IT, University of Engineering and Technology, Jalozai Campus, Pakistan[(4)]

***Abstract*—Securing crucial information is always considered as one of the complex, critical, and a time-consuming task. This research investigates a significant threat to the security of a network, i.e., selective forwarding attack. Protection of information is considered as the main stimulating task in the design of an information system for an organization. The research work proposes a framework that detects the selective forwarding attacks and computes the harmful hosts residing an ad-hoc structure. Our solution is further split into two phases: initial phase is the detection of selective forwarding attacks and the second phase performs the identification of malicious nodes. Performance of the proposed model is evaluated based on the network throughput, which is for the enhancement of security. Simulation of the proposed model is performed using NetLogo and the results show an improvement of 20% in throughput of the network.**

***Keywords*—Ad-hoc on-demand distance vector; control ACK; mobile ad-hoc network; network throughput**

I. Introduction

Ad-hoc network is considered as one of the most emerging technologies in today's world. The unique ad-hoc mesh structure of a network is the latest wireless networking model of roving hosts. In an ad-hoc network, the hosts rely upon one another to enable and maintain the entire network communicating and linked together. The ad-hoc networking model has achieved a lot of attention in the industry of information technology as well as in academics. The ad hoc mesh is most developing technologies in the information technology world. Significant research has been conducted in emerging technology of mobile ad-hoc network (MANET).

The use of MANET upon people's day-to-day life style has greatly developed with the passage of time. Thus, in response it has created an immense requirement for a secure ad-hoc structure. Greater amount of investigation and research is focusing upon constructing and modeling efficient and safe ad-hoc network [1], [2]. To provide defense from malicious hosts, different researchers are working specifically to the challenges concern to security of MANETs [11].

The ad hoc structure is built with the help of a number of mobile nodes that are connected wirelessly and they cooperate with each other. These networks transfer the information and data by using the multi-hop forwarding techniques. The deployment for a spectacular MANET structure is very useful into such area where the pre-deployed infrastructure is not supportive. There are several recent works on the security of MANETs but most of them have failed due to different aspects including network throughput, performance, etc. [9]. With the passage of time as the user of the computing technology is dynamically growing, the threat to the computing technology has increased as well, which demands for security requirement. Increasing users of computing technology has also created the problem of finding the loopholes.

To develop a safe and secure routing protocol for an ad-hoc structure is a daunting task owing to its distinctive mesh properties such as missing of central control, quick host mobility, continuously change of topology, safe working environment, and accessibility to resources [10]. A MANET is a group of roving hosts that can create a neighborhood for themselves. It is possible that they leave an area open. Therefore, it is crucial to have a safe and reliable exchange of data within MANET [12].

A. Key Contributions

- The proposed system presents an efficient framework, which detects selective forwarding attacks and identifies malicious nodes in the network.
- Thorough experiments are performed for the verification and validation of the proposed solution. Malicious hosts are created randomly for testing in the simulation environment.
- The harmful hosts are positioned in the forwarding path of simulation environment. The control packet and control ACK is added to the ad hoc on-demand distance vector (AODV) routing protocol for the verification and validation of our proposed framework.

B. Paper Organization

Rest of the paper is organized as follows: Section II provides the prior work. Section III discusses the proposed solution, control packet/ control ACK, and different cases. Section IV gives evaluation of the proposed solution based on the experiments. Finally, Section V concludes the paper and highlights the future work.

II. Previous Routing Mechanisms

The number of information technology users are dynamically increasing. Consequenlty, the issue of the security is increasing. There are many types of protocols, which include SRP [5], SEAD [6], and SAODV [7]. These routing protocols have been addressing the security attacks and have presented a different solution to counter security

attacks. Most of these protocols use different authentication techniques including public key management, asymmetric key management, and many other authentication techniques.

The secure key management scheme was given by [2], which was based on the threshold cryptography. The scheme worked efficiently when it had to deploy in large scattered areas. The mobiles nodes contact the servers. A refreshing scheme was used to counter the mobile node adversaries. Scheme in [8] was based on simple architecture where all nodes were considered as servers. Main advantage of the scheme was that it was highly efficient and secure while performing local communication. The scheme reduced security in case when mobile nodes were not physically protected.

Several security routing protocols and framework were introduced in the past years such as SEAD, which was modeled and established for wireless ad-hoc mesh for the distance vector routing. There is a number of researchers who have been extending these techniques on the simulation of different goals. In [1], the design and evaluation of efficient secure AODV routing protocols were mainly focused. A protected ad-hoc structure for routing stands upon frame of "destination-sequenced distance-vector" routing protocol. The work restricted CPU working capacity and protection towards the attacks for the service denial where attacker tries to force other nodes capture excess processing time or bandwidth of the network [3].

In [6] authors presented a complete survey on the solutions and challenges within the security perspective of the wireless network and discussed some improvements to overcome these challenges. The provided solution can be simulated on different techniques. To address a number of challenges as identified in the survey, the survey was simulated around key management techniques, routing protocols, and securing challenges involved in it.

The prior work presented the intrusion detection in order to resolve a number of issues, which have been presented in the survey. The research study in [3] presented a new approach inspired by trust model and clustering algorithm. The solution utilized the certificate authority (CA) for securing the information in the MANET. The solution utilized the self-organization security and PGP (trust model) to secure ad-hoc network. In the solution, all the cluster nodes hold the CA and are registered to the specific authority that authorities issue the certificates to the cluster nodes.

III. Proposed Solution

The solution proposed is divided into two phases; a) to find and b) localize selective forwarding attacks on MANET. In the first phase, selective forwarding attacks are detected. Since a mesh of random numbers is needed, it is generated for the nodes of source and destination. The AODV protocol route requests are flooded in entire MANET. Since a packet counter is required, it is maintained in each node so that a track of all packets sent is kept and received by the node. Second phase of the proposed solution provides a detection scheme, which is based on two different packets. The given method "the control packet and the control ACK" is utilized in the detection scheme.

A. Control Packet and Control ACK

The proposed solution contains the new control packet. This packet is added to the data packet in the protocol of AODV. Main goal is to add these packets to identify the selective forwarding attacks and malicious nodes that are presented in the network. The control packet and control ACK (acknowledge) packet contain the parameter including final hash, hash function, hash field, destination ID and source ID. The control packet contains the parameters given in Table I.

TABLE I. Control Packet and Control Ack

Control Packet & Control ACK				
Final hash	Hash function	Hash field	Destination ID	Source ID

Table I presents the structure of control packet and control ACK. The source ID filed contains the information about source node from where the packet is generated and the destination ID field contains the information about the destination node. Total number of hops is carried from source to destination by the hash. Hash function is used to compute hops between destination and source, which is stored in final hash. In the end, the final hash value is compared with the security value stored in hash field. The hash chain is implemented on each packet to make the communication secure. The control packet is sent with each data packet.

Algorithm 1 Retrieve hash field value algorithm

1: **If** (Final – Hash = F Hop Count (Hash)) **then**
2: Retrieve the packet count value in the Hash field of the control packet
3: **else**
4: Drop the control packet

Algorithm 1 is used by the final node, which accepts the control packet and accomplishes the operation as per steps given in Algorithm 1. There are three cases of control ACK; a) positive control ACK, b) negative control ACK and, c) no control ACK. Table II "Cases of Control ACK" presents the three cases of control ACK. In the first case, hop count is equal to the detection threshold and as a result positive control ACK is sent from destination to source node in order to send data packet for communication. This case has no attacker and thus communication occurs in a safely manner. In the second case, the hop count is less than the detection threshold and as a result destination sends negative control ACK to source host. The negative control ACK mentions the presence of the potential attacker in the forwarding path to the source host. While in the third case, there is no control ACK received by the source node from the destination, demonstrating the existence of attacker in the forwarding path that has dropped the control ACK or has dropped control packet; hence, destination did not receive any packet.

TABLE II. CASES OF CONTROL ACK

Case I	Case II	Case III
Positive Control ACK from Destination	Negative Control ACK from Destination	No Control ACK from Destination
Count (destination packet) = detection threshold	Count (destination packet) < detection threshold	⦿ Condition I Malicious host drops the control ACK, which is send by the destination. ⦿ Condition II Malicious host drops the control packet, as it doesn't reach destination, so destination does not reply with any control ACK.
In case I, the control ACK received by source host.	In case II, control ACK received by source host.	In case III, no control ACK received by the source node.
No presence of attacker	Presence of attacker	Presence of attacker

B. Detection of the Malicious Hosts

When it is detected that a malicious node is present, the source node begins querying all hosts, which are present in the forwarding path and then gets a value of the packet counter. A counter frequency is utilized to choose the intermediate nodes in the way between destination and source nodes. A suitable value of the counter frequency could be computed by using mesh topology experiments [4]**.** Table III presents two different cases of malicious node detection.

If the malicious node is noticed then the source node forwards the error packet in order to update all the hosts, which are existing in neighborhood about the harmful host. Specific node is dropped from the routing table and in future, during the route discovery, the malicious nodes are not considered again. The removal of harmful host from neighborhood enhances overall network performance of the network as the packets of the malicious nodes are no longer flooding in the network

TABLE III. CASES OF MALACIOUS NODE DETECTION

Case I	Case II
Malicious host drops all packets.	Malicious host drops few packets.
No control ACK received	Negative control ACK to source
Malicious node detected	Malicious node detected

IV. EVALUATION

A. Detection Threshold

In this subsection, analysis of the threshold is performed. Detection of the threshold is designed upon metric of expected transmission count (ETX). The ETX calculates total number of counts, which are needed for the successful delivery of a packet between a source and destination. Total number of the count also includes the retransmitted packets. Table IV describes the threshold parameters.

TABLE IV. THRESHOLD PARAMETER

Symbol	Parameter	Description
D_f	Forward delivery	Probability of the packet deliver successfully.
D_r	Reserve delivery	Probability of the ACK packet received successfully.

The ETX link is computed by using (1).

$$\mathrm{ETX} = \frac{1}{D_f - D_r} \quad (1)$$

B. Simulation

The AODV protocol is simulated on the MANET based in real-time environment. Ad-hoc network environment is deployed. The nodes detect the environment and rain, speed, average humidity, wind speed, temperature and find fire weather index (FWI) based on this parameter. Network throughput in kbps is used as an evaluation metric for the proposed solution. There are 35 nodes deployed in the forest fire simulation model. The AODV protocol is used for communication between these mobile nodes. The data packet of each node contains the information of current temperature (T), rain (R), wind speed (WS), and average humidly (H). Harmful hosts are randomly created in the environment. These harmful hosts are positioned in the forwarding path. The control packet and control ACK are added to the AODV routing protocol for verification and validation of the proposed model. The timeout is set to 2 units before the initialization of the lead-off node. The ETX metric is integrated into the AODV protocol.

C. Performance Results

Performance of the proposed solution was evaluated and analyzed based on the network throughput. The detailed discussion of the experiments performed and their corresponding results has been provided. Two different experiments have been simulated based on different scenarios and parameters. The harmful hosts are also added in the network with the context of the experiment so that the right performance and efficiency can be calculated by the help of the respond time of the simulation environment.

1) Experiment no. 1: The forwarding path between source node and destination node has a single attacker. Within this experiment, attacker is randomly deployed in the path of selective forward routing. In the simulation environment, two observations are made. First is the network throughput and the second is detection. Network throughput is decreased as there is a presence of malicious nodes. As the malicious node interrupts with the communication held between the nodes of the network, the throughput of the network drops, which can be seen in Fig. 1

In order to define and measures the results more accurate, the experiment was considered and executed for more than ten times and based on that simulation the following graph has been generated. During simulating environment, bit error rate is also considered while calculating throughput in the context

of this research and errors have also been considered that occur in the transmission of digital data and based on the analysis, the overall performance is computed.

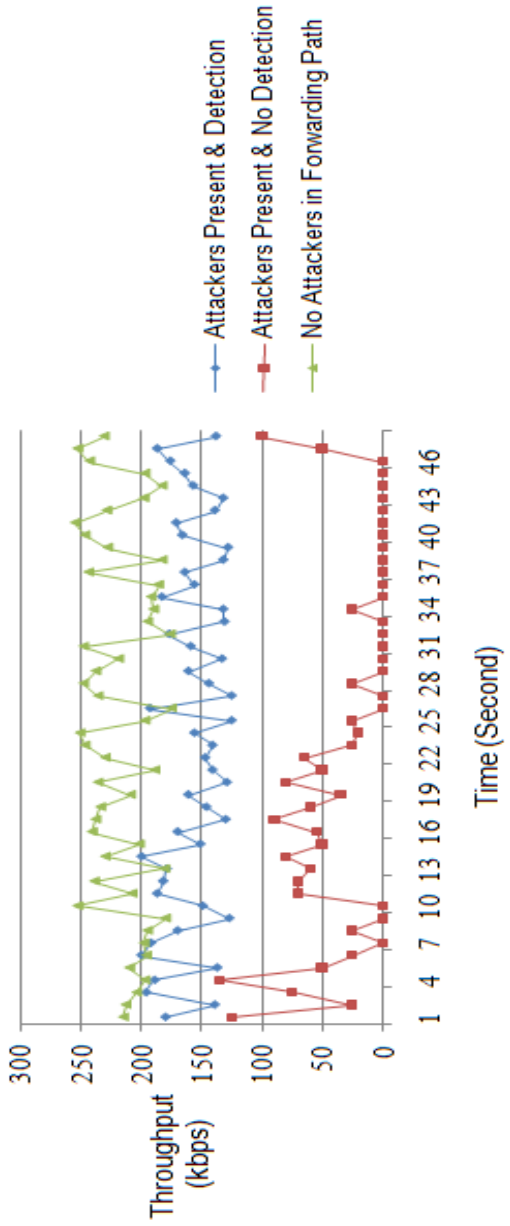

Fig. 1. Single attacher present in the forwarding path.

The time is considered on the X-axis and the network throughput is considered on the Y-axis. It can be observed from the above graph as the time passes the network throughput increases. The graph in Fig. 1 that is mentioned in the experiment is generated from Table V, which contains different values of “attacker present and detection”, “attacker present and no detection” and “no attacker in forwarding path”.

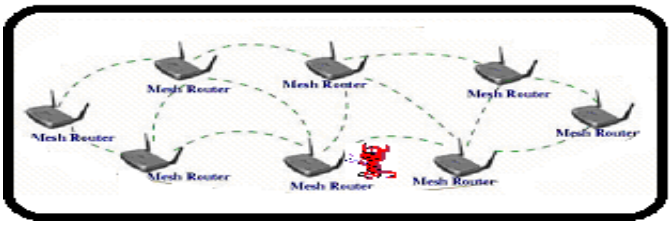

Fig. 2. Single malacious node in the forwarding path.

TABLE V. THROUGHPUT OF THE NETWORK IN CASE OF A SINGLE ATTACKER

Attackers present & detection (kbps)	Attackers present & no detection (kbps)	No attackers in forwarding path (kbps)
182	125	246
142	25	249
194	75	191
129	135	238
151	50	192
162	25	240
176	0	186
125	25	251
168	0	208
161	0	222
182	70	220
148	70	201
141	60	243
142	80	181
194	50	245
127	55	255
155	90	251
154	60	231
172	35	184
150	80	233
178	50	219
186	65	205
200	25	209
200	20	243
164	25	229
153	0	225
150	0	235
177	25	235
186	0	206
180	0	235
156	0	227
127	0	244
192	0	191
187	25	230
166	0	212
145	0	204
133	0	222
145	0	195
143	0	219
192	0	252
148	0	199
154	0	180
137	0	192
159	0	217
132	0	233
137	0	181
187	50	241
144	100	252

Fig. 1 has three different graphs, which are used to show the network performance based on the network throughput. The green graph shows different values of the throughput when there is no attacker present in the forwarding path; the throughput is the highest in this case. The red graph shows the values of throughput when network has the presence of an attacker but not detected; the throughput is the lowest in this case. While the blue graph shows values of the throughput when attacker was spotted and then removed from neighborhood, which results in better network throughput than the case when there is no detection of the attacker. The green and red graphs were obtained by simple AODV while blue graph was obtained by the implementation of the proposed solution. In Fig. 2, forwarding path has a single malicious node, which attempts selective forwarding attack.

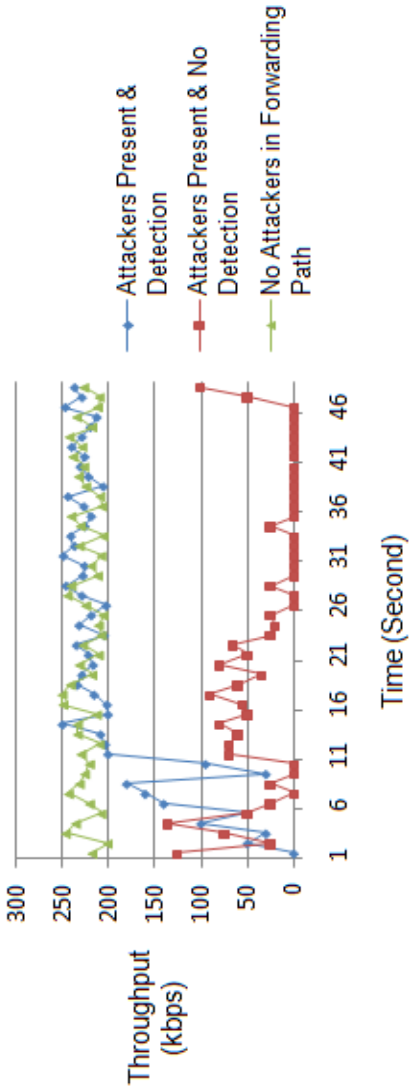

Fig. 3. Multiple forwarding paths between source node and destination node have colluding attackers.

2) Experiment no. 2: In mutiple forwarding paths between source and destination, colluding attackers are present. In this experiment, there were more than two attackers randomly.

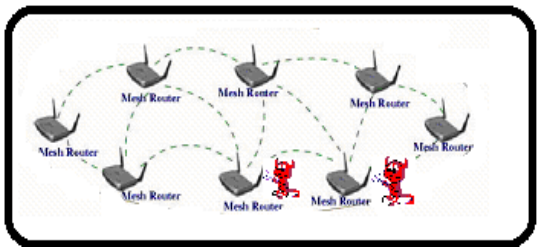

Fig. 1. Colluding malicious nodes in the multiple forwarding paths.

TABLE VI. THROUGHPUT OF THE NETWORK IN CASE OF TWO ATTACKERS

Attackers present & detection (kbps)	Attackers present & no detection (kbps)	No attackers in forwarding path (kbps)
0	125	242
50	25	238
30	75	209
100	135	232
50	50	205
140	25	224
160	0	210
180	25	230
30	0	243
95	0	239
200	70	243
237	70	238
202	60	235
224	80	212
242	50	227
248	55	223
206	90	204
219	60	210
231	35	207
228	80	210
204	50	226
204	65	203
204	25	222
207	20	240
244	25	247
218	0	234
214	0	209
238	25	232
248	0	236
212	0	212
240	0	219
234	0	233
225	0	241
221	25	244
213	0	238
234	0	232
204	0	239
207	0	231
250	0	214
205	0	250
203	0	238
210	0	241
247	0	244
221	0	230
211	0	212
240	0	244
230	50	218
241	100	249

Selected and placed in between multi path of selected forwarding routing. Network throughput is increased as the malicious nodes were detected. In order to obtain accurate results, the experiment was executed for more than ten times and based on that simulation; the graph in Fig. 3 is generated. Bit error rate and errors occur in the transmission have also been considered and based on analysis, the overall performance is calculated.

The graphs in Fig. 3 are generated from the data of Table VI, which contains different values of "attacker present and detection", "attacker present and no detection" and "no attacker in forwarding path". Fig. 3 shows that throughput of network increases after the specific time interval. The new route request is generated and the malicious nodes are removed from the routing table. Network performance is improved after specific time interval. In initial phase, performances was low but after detection of attackers within a time interval of 0 -7s new routes were identified in network and the malicious nodes were removed. Time (seconds) is considered on the X- axis and network throughput (kbps) is considered on the Y-axis. In Fig. 4, two malicious nodes are present in the multiple forwarding paths attempting the selective forwarding attack.

D. Network Overhead

The control packet send with each data packet increases the system's algorithm complexity and processing time, which results in network overhead. Although the control packet design has a slight network overhead but after the detection and elimination of the malicious nodes, their packets are no longer floating in the network plus there is also no need to resend the dropped packet hence increasing the overall performance and reducing the overhead of the network.

TABLE VII. SUMMARIZED OBSERVATIONS

Experiment No.	**Scenario**	**Observation**
1.	When there is a single attacker in the forwarding path of the network	Network throughput is decreased as there is a presence of the malicious nodes.
2.	When there are more than one attackers present in multiple forwarding paths between destination and source	Performances of the network throughput increases after the specific time interval.

Table VII summarizes the observations made in the experiments performed for the evaluation of the proposed system.

V. CONCLUSIONS

We developed and simulated a framework for the detection of selective forwarding attacks using MANET technologies. A network environment is deployed and several experiments were performed for the verification and validation of the proposed solution. For the testing purpose, malicious nodes were randomly created in the environment. These malicious nodes were positioned in the forwarding path of the simulation environment. The control packet and control ACK are added to the AODV routing protocol during evaluation of the system. The proposed solution can be applied to the protocols such as DSR and DSDV. There are some parameters such as network overhead and threshold detection, which can be done in future work.

REFERENCES

[1] J. Jubin and D. Tornow, "The DARPA packet radio network protocols," Proceedings of the IEEE, 75(1), pp. 21–32, 1987.

[2] L. Zhou and Z. Haas, "Securing ad hoc networks," IEEE Network Magazine 13(6):, pp. 24–30, 1999.

[3] N. Schacham and J. Westcott, "Future directions in packet radio architectures and protocols ," Proceedings of the IEEE, 75(1), pp. 83–99, 1987.

[4] S. Capkun, L Buttyan, and J. Hubaux , "Self-organized public-key management for mobile ad hoc networks," IEEE Trans Mobile Computer 2(1), 2003.

[5] P Papadimitratos and Z Haa, "Secure routing for mobile ad hoc networks," Proceedings of the SCS communication networks and distributed systems modeling and simulation conference (CNDS 2002), 2002.

[6] D Johnson, A. Perrig, and Y. Hu, "SEAD: secure efficient distance vector routing in mobile wireless ad-hoc networks," Proceedings of the 4th IEEE workshop on mobile computing systems and applications (WMCSA'02), pp. 3–13, 2002.

[7] M. Zapata, "Secure ad hoc on-demand distance vector (SAODV)," Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.

[8] H. Luo and S. Lu, "URSA: ubiquitous and robust access control for mobile ad-hoc networks," IEEE/ACM Trans Networking 12(6), pp. 1049–63, 2004.

[9] M. P. Shelke, A. Malhotra and P. Mahalle, "A packet priority intimation-based data transmission for congestion free traffic management in wireless sensor networks," Computers & Electrical Engineering, vol. 64, pp. 248-261, 2017.

[10] V. K. Saurabh, R. Sharma, R. Itare and U. Singh, "Cluster-based technique for detection and prevention of black-hole attack in MANETs," in International conference of Electronics, Communication and Aerospace Technology (ICECA), 2017.

[11] L. Baghel, P. Mishra, M. Samvatsar and U. Singh, "Detection of black hole attack in mobile ad hoc network using adaptive approach," in Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of, 2017.

[12] D. Gayathri and S. J. Raman, "Pltrust AODV: Physical logical factor estimated trust embedded AODV for optimised routing in Manets," in Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on, 2017.