World Engineering & Applied Sciences Journal 6 (1): 09-14, 2015
ISSN 2079-2204

DOI: 10.5829/idosi.weasj.2015.6.1.22020

Advanced Secured Model for On-Demand Distance Vector Routing Protocol in Manet

[1]R. Vijayakumar and [2]K.R. Shankar Kumar

[1]Department of Computer Science and Engineering,
Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India
[2]Department of Electronics and Communication Engineering,
Ranganathan Engineering College, Coimbatore, Tamilnadu, India

Abstract: A mobile ad-hoc network is a group of mobile nodes which can communicate between them without the help of any centralized infrastructure. It consists of number of mobile nodes with exceptional quality of self-managing and self-organizing network. Military operations and disaster management are the important applications of MANET. In preventing routing attacks routing protocols plays a significant role. Security attacks can be initiated towards any layer of the stack protocol. MANETs distinctive characteristic like dynamic network topology, battery power and limited bandwidth makes routing an challenging task. Several researches are done in this area and many efficient routing protocols were proposed. But due to the presence of malicious node, these protocols are vulnerable to attacks. Therefore for establishing the attractive MANET, security is a major concern. In this paper we proposed an Advanced secured model for On-demand Distance vector routing protocol, which is highly secured against Denial of Service (DoS) attack and Blackhole (BH) attack. This method can provide highly secured routing with better performance than the typical AODV in terms of packet delivery ratio, normalized routing load and the average throughput.

Key words: MANET · Security · DoS attack · Blackhole attack · Packet Buffer

INTRODUCTION

MANETs with collection of mobile nodes communicate through wireless links. The mobility of nodes makes the network topology to change rapidly and unpredictable. Route discovery process in MANET is the major function and to transfer data packets routes are discovered from source to destination node. There are 3 classes of routing in MANET namely Proactive, Reactive and hybrid protocol [1, 2]. In MANETs proactive are the table driven protocols where route is maintained at each node to every other node, but this protocol is less preferred because of its processing power, limited memory and battery capacity. In wireless ah-hoc networks, Reactive routing approach is more popular because of its on-demand and less overhead nature [3].

Dynamic Source Routing (DSR), ad hoc on-demand distance vector (AODV) and associativity based routing are the popular reactive routing protocols [4-6]. Hybrid protocols are the combination of both proactive and reactive protocols, in this protocol, when route is initialized proactive routing is used to store the route and to deliver the packets to its destination node reactive broadcasting is used. Among the hybrid protocol, Zone Routing Protocol (ZRP) is the most popular one [7]. Since the MANETs are deployed in harsh conditions, the uncontrolled behavior and network malfunctioning probability is very high. This makes the network vulnerable to attacks like black hole attack, Denial of Service (DoS) attacks and grey hole attack [8]. By introducing the neighboring nodes trust scores, the nodes which are misbehaving can be avoided in the route discovery process. The integrity of the data received at receiver node will be improved by using the trust based routing protocol [9-11]. The stable and secure design of routing protocols is an current research area in MANET.

Corresponding Author: R. Vijayakumar, Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India.

To sustain the reliability of network operations the nodes cooperation is more important [12]. Though most nodes are malicious or selfish, protecting the routing protocols against various attacks secure routing protocol is required. In this paper, we proposed an enhanced secured model for On-demand Distance vector routing protocol. This proposed model provide security against Denial of Service (DoS) and Black Hole (BH) attack.

Security Concerns: In MANET security is a vital component for its extensive use. Continuous and dynamic changing network is a MANETs unique characteristic. Bandwidth and the limited battery power are the resource constraints that make it difficult for the conventional networks to use the existing security system directly [13]. MANETs attacker by actively or passively can violate entire goals of security like availability, integrity, confidentiality, access control, non-reputation and authentication [14]. Among the various attacks in this paper Denial of service (DoS) and Black hole (BH) attacks are focused in this paper.

Deniel of Service (DOS) Attack: This attack have termed as a most perturbing problem in MANET. In an environment like military, it is extremely dangerous to have a successful DoS attack [15, 16]. The restriction put by Route request rate limit can be overridden by the malicious node in the DoS attack by disabling or increasing it. The RREQ_RATELIMIT parameter may set to choose a very high value by the adversary node, which leads the network with flooding of fake RREQ and leads to DoS attack. The node in the DoS attack cannot truly serve other nodes owing to the network load forced by false RREQ packets. This attack could deadly affect the entire discovery process of the network.

Black Hole Attack: The malicious node hangs around for neighbor node to begin a route request packet in the BH attack. Immediately after node receiving the RREQ packets, it sends fake RREQ with modified high series number. This makes source node to think that node having a new routes towards the destination. The received RREP packet from other nodes is ignored by source node and over the malicious node it starts sending the packets. The malicious node acquire entire route towards itself. It ingests all data packets by not allowing any packets to forward anywhere [17-19].

Aodv Fundamentals: AODV is a most popular reactive routing protocol which has been researched dynamically [20, 21]. It has phases of route maintenance, route discovery and neighbor maintenance. When data packets to be send from source node S to a destination node D, the route discovery phase is initiated by broadcasting RREQ packets to its neighbor nodes.

The RREQ packets received to immediate neighbors will be rebroadcasted to their own neighbors, until the RREQ packets reaching the destination node D it continuous to broadcast. Ahead of receiving RREQ message, the RREP message is replied back from node D to node S. The messages are replied back to the same route where route request messages are received. The RREQ messages arrived late will be ignored and the date transmitted through this route can be believed as discovered path. In addition, intermediate nodes are enabled by AODV that have enough fresh routes to send and generate RREP to source node.

Generally AODV is scalable and efficient protocol, but has no intrinsic security system. Since this protocol is completely security vulnerable, it is easy for attacker to attack the routes. In AODV vulnerabilities present are due to hop count decrease and sequence number increase in RREQ/RREP, RERR message forging, attacker possibilities in impersonating source node S and destination node D by fake RREQ IP address.

Proposed Secured Model: In this paper, the description of the proposed method including its framework, architecture, maintenance, route discovery and attack prevention is described. The proposed protocol has two phases namely route maintenance and route discovery phase. The proposed design has three modules namely observing directly, promiscuous observation of modes and establishment of advanced secured route discovery, route maintenance and attack protection. The purpose of the proposed method is to protect from malicious attack like DoS and the Black hole attack.

The protection is provided by calculating the neighbors trust value in our proposed design. By introducing the Packet Buffer (PB) and Node Trust Table the AODV routing protocol is modified to design a proposed secured model. The information of malicious node and neighbor node is stored in NTT. Neighbour node ID is stored in each node and calculates that node trust value based on the observation of the packet as shown in equation below.

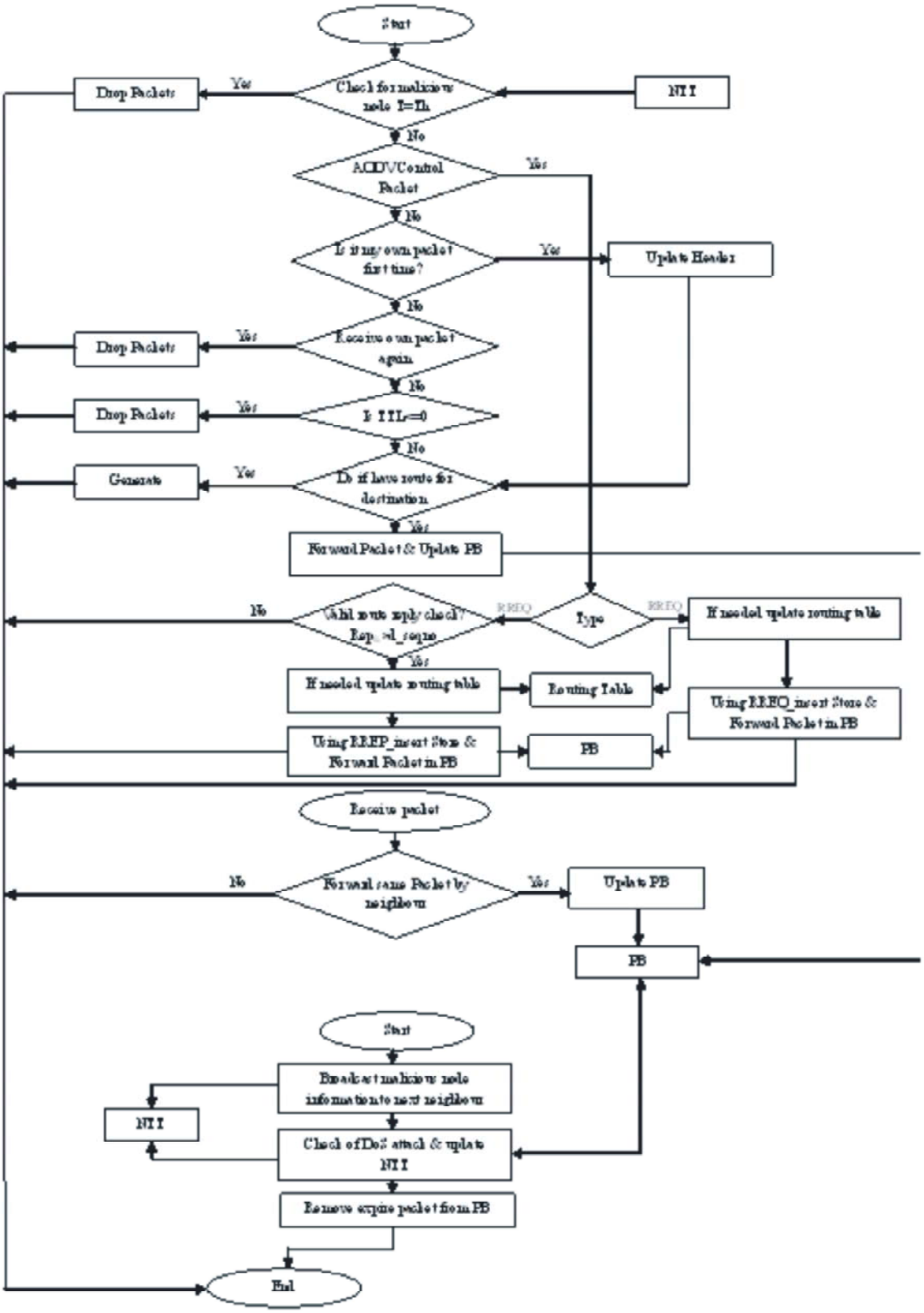

Fig. 1: Flow diagram of the proposed method

$Nt_v = MAX(0, MIN(1, K * T_{XYi}) + (1– K) * (T_{XYi} + R_C)))$

In the above equation, K represent constant (K=0.93) and R^C may represent anyone of the constant like RREQ constant, RREP constant, Data constant and Black hole constant. If RREQ constant and RREP constant are equal to 0.3, then it is success and if it is equal to -0.3, then it is failure. Similarly for Data constant, if it is equal to 0.4, it is success and if it is less than -0.4, it is failure. Initially node x trust for y at i_{th} event (T_{XYi}) is equal to 0.5 by default and gets updated on failed and successful transmission. Black hole constant is set to -7.2 and its minimum trust value and maximum trust value is set as 0 and 1 respectively. The value of threshold is set as 0.5 and packets will be dropped if the node having trust value of less than 0.5.

Packet buffer (PB) includes 3 types namely PB_DATA, PB_RREQ and PB_RREP. This Packet Buffer was used to store data packets and control packets, sent by node itself or forwarded from other received node, based on Packet Buffer timer and promiscuous mode. Both while sending and forwarding of RREQ, RREP and DATA of each node to next node, it store the data and control packets in its Packet Buffer.

Packet Buffer has functionality to delete, insert, update, search, print table and access entries of Node Trust Table to update neighbors trust value based on observation. All expired packet will be deleted from the buffer at the predefined interval.

So the network is completely secured in the proposed method based on the trust value. In this paper secured routing protocol is proposed to secure and maintain the route discovery process from different attack and to safely transfer the data packets over the network as shown in Figure 1.

RESULT

The performance of the proposed method is measured using the simulator (NS-2) and the result is compared with AODV. Average throughput, packet delivery ratio and normalized routing load are considered to demonstrate the proposed method. In a network, a rate of data packets successfully transmitted in unit time is called as average throughput. Packet delivery ratio is defined as the ratio of no. of data packets received successfully at the destination over the packets sent by the sources and normalized routing load is defined as the

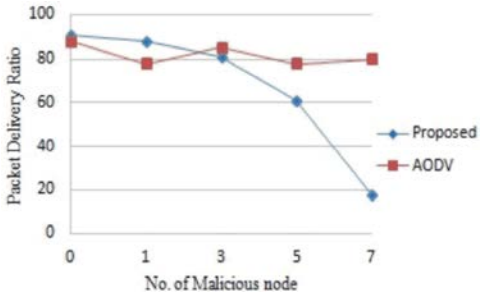

Fig. 2(a): Packet delivery ratio comparison

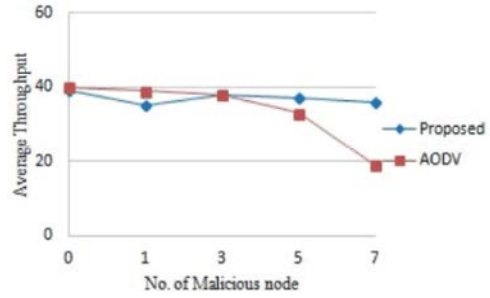

Fig. 2(b): Average through put comparison

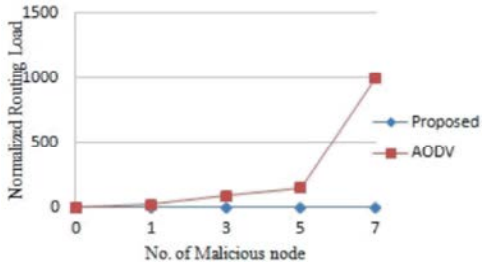

Fig. 2(c): Normalized Routing Load comparison

Fig. 2: Result of DoS attack

ratio of no. of routing packets sent via network to that of no. of received data packets. The performance of the proposed secured method is evaluated using NS-2.35 and compared it with the AODV. The result is evaluated with seven malicious nodes on the routing path.The impact under Denial of Service attack on average throughput, Packet delivery ratio and normalized routing load of the proposed secured model and comparison with AODV is showed in Figure 2.

The simulation is performed for the network with one to seven malicious nodes. In the network if there is no malicious node, the performance of both proposed and AODV are similar. In the presence of malicious node, our proposed secured protocol can maintain the average throughput constantly above 32, but in AODV it fall significantly as shown in Figure 2(a). Packet delivery ratio

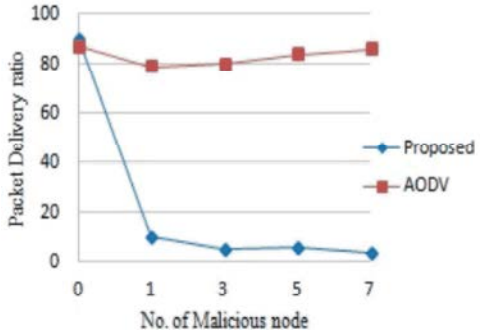

Fig. 3(a): Packet delivery ratio comparison

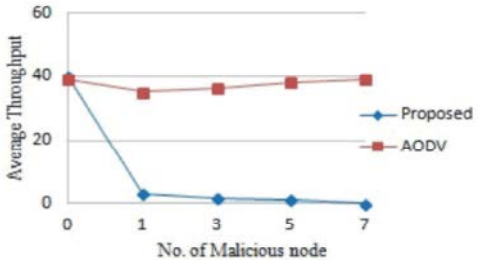

Fig. 3(b): Average throughput comparison

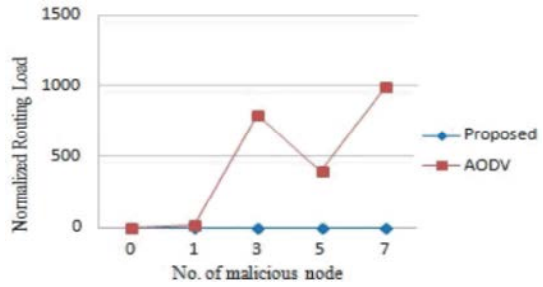

Fig. 3(c): Normalized Routing Load comparison

Fig. 3: Result of black hole attack

is always maintained constantly higher than 80%, but it keeps falling continuously in AODV as shown in Figure 2(b). Similarly for the normalized routing load with increasing malicious nodes AODV will entirely increase or decrease, but in the proposed model it is maintained small as shown in Figure 2(c).

The impact of blackhole attack of our proposed secured protocol is shown in Figure 3.The simulation is carried out for average throughput, packet delivery ratio and normalized routing load and the result is compared with the typical AODV.In the presence of malicious node, our proposed secured protocol can maintain the average throughput constantly above 30, but in AODV it

Fall significantly even in the occurrence of one malicious node as shown in Figure 3(a). Packet delivery ratio is always maintained constantly from 80% to 85%, but in AODV it drop down to 5% as shown in Figure 3(b). Similarly for the normalized routing load, the proposed secured protocol is always small, while in AODV I keeps on fluctuating as shown in Figure 3(c).

CONCLUSION

Since MANET does not use any specific infrastructure, a node present in it should be secured and supportive. The attacks more often targets the topology related routing information or control messages. In this paper, advanced secured model for On-demand Distance vector routing protocol is proposed which facilitates the route discovery security and its maintenance. Even in the presence of increasing malicious node in MANET, this proposed secured method is able to deliver the packets to the destination. The performance is evaluated by considering the average throughput, normalized routing load and packet delivery ratio against DoS attack and Blackhole attack. When compared with other existing methods this proposed secured model is more efficient.

REFERENCES

1. Andel, T.R. and A. Yasinsac, 2007. Surveying security analysis techniques in manet routing protocols, Communications Surveys & Tutorials, IEEE, Fourth Quarter, 9(4): 70-84.
2. Papadimitratos, P. and Z. J. Haas, 2006. Secure data communication in mobile ad hoc networks, IEEE Journal on Selected Areas in Communications, 24(2): 343-356.
3. Hui Xu, Xianren Wu, H.R. Sadjadpour and J.J. Garcia-Luna-Aceves, 2010. A unified analysis of routing protocols in MANETs, Communications, IEEE Transactions on, 58(3): 911-922.
4. Shankar, S. Varaprasad and H.N.G. Suresh, 2014. Importance of on-demand modified power aware dynamic source routing protocol in mobile ad-hoc networks, Microwaves, Antennas & Propagation, IET, 8(7): 459-464.
5. Nakayama, H. Kurosawa, S. Jamalipour, A. Nemoto and N.Y. Kato, 2009. A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks, Vehicular Technology, IEEE Transactions on, 58(5): 2471-2481.

6. Masoud, F.A.M., S.A. Shaar, A. Murad and G. Kanaan, 2006. Enhanced routing re-constructionmethod for the associativity based routing protocol form obile ADHoc network (MANET), The American Journal of Computer Science, 2(12): 853-858.
7. Haas, Z.J. and M.R. Pearlman, 2001. The performance of query control schemes for the zone routing protocol, Networking, IEEE/ACM Transactions on, 9(4): 427-438.
8. Karjee, J. and S. Banerjee, 2008. Tracing the Abnormal Behavior of Malicious Nodes in MANET, Wireless Communications, Networking and Mobile Computing. 2008. WiCOM '08. 4th International Conference on, 1(7): 12-14.
9. Jin-Hee Cho Swami and A. Ing-Ray Chen, 2011. A Survey on Trust Management for Mobile Ad Hoc Networks, Communications Surveys & Tutorials, IEEE, Fourth Quarter, 13(4): 562-583.
10. Abdelaziz, A.K. Nafaa and G.M. Salim, 2013. Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks, Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on, 10(12): 693-698.
11. Jie Li, Li Ruidong and J. Kato, 2008. Future trust management framework for mobile ad hoc networks, Communications Magazine, IEEE, 46(4): 108-114.
12. Cheng Yong, Huang Chuanhe and Shi Wenming, 2007. Trusted Dynamic Source Routing Protocol, Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on, 21(25): 1632-1636.
13. Khurana, S. Gupta and N.N. Aneja, 2006. Reliable Ad-hoc on-demand Distance Vector Routing Protocol, Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on, 23(29): 98-98.
14. Chien-Chung, Shen, Srisathapornphat and C.C. Jaikaeo, 2003. An adaptive management architecture for ad hoc networks, Communications Magazine, IEEE, 41(2): 108-115.
15. Hejmo, M. Mark, B.L. Zouridaki and R.K.C. Thomas, 2006. Design and analysis of a denial-of-service-resistant quality-of-service signaling protocol for MANETs, Vehicular Technology, IEEE Transactions on, 55(3): 743-751.
16. Jhaveri, Rutvij H. Patel, Ashish D. Dangarwala and J. Kruti, 2012. Comprehensive study of various DoS attacks and defense approaches in MANETs, Emerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference on, 25(31): 13-14.
17. Payal N. Raj and Prashant B. Swadas, 2009. DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET, IJCSI International Jtheynal of Computer Science Issues, 2.
18. Dokurer, Semih, 2006. Simulation of Black hole attack in wireless Adhoc networks. Master's thesis, AtılımUniversity.
19. Alem, Y.F. Zhao and Cheng Xuan, 2010. Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection, Future Computer and Communication (ICFCC), 2010 2nd International Conference on, V3-672, 676: 21-24.
20. Perkins, C., E.B. Royer and S. Das, 2003. Ad hoc on demand distance vector (AODV) routing, presented at IETF RFC 3561.
21. Abusalah, L. Khokhar and M.A. Guizani, 2008. A survey of secure mobile Ad Hoc routing protocols, Communications Surveys & Tutorials, IEEE, Fourth Quarter, 10(4): 78-93.