International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 5 Issue 11 November 2018

Modified Trust Mechanism for detection and prevention of DDoS Attack under MANET Scenario

Varsha Kushwah[1], Prof. Shiva Bhatnagar[2]
Department of Electronics and Communication, PCST Indore[1, 2]
varsha.kushwah.1994@gmail.com[1]

Abstract: *In this paper, we design and formulate a novel trust-based routing protocol to secure nodes from attack i.e. Distributed denial-of service attack, in mobile ad hoc networks (MANETs). The innovative approach is employing the idea of a trust model in the network layer of MANET so as to achieve security in mobile ad hoc networks cost-effectively. The main security threat on MANET could be a DDoS attack. DDoS attack has the flexibility to make immense quantity of unwanted traffic. as a result of this the licensed user cannot used the resources properly. It is terribly laborious to notice and management the DDoS attack as a result of massive scale and complicated network environments. The scope of this paper is to study the effects of DDos attack in Ad hoc On-demand Distance Vector (AODV) routing protocol. The new protocol, called TAODV and prevention this attack using security AODV and (T-AODV) Comparative analysis of DDoS attack for both protocols is taken into account. The impact of Node DDos attack on the performance of MANET is evaluated finding out which protocol is more exposed to the attack and how much are the contact of the attack on both protocols. The dimensions were in use in the beam of packet delivery ratio, throughput, end-to-end delay, normalized routing load and residual energy. Simulation is done in Network simulator tool 2 (NS-2).The values of opinions are updated during a routing information exchange process. If a node performs healthy behaviors, its credibility from the viewpoints of other nodes is increased; otherwise, the credibility will be decreased, and this node will be eventually denied by the whole network. We also devise an effective recommendation trust mechanism to exchange the trust information among nodes. The performance of our protocol is evaluated through analyses and simulations. The results demonstrate that the whole MANET system.***

Keywords: *MANET, DDoS attack, AODV, and TAODV Routing Protocols, NS-2.35.*

1. INTRODUCTION

Mobile Ad-hoc Network could be a self-configuring infrastructure less network of mobile device that is connected through wireless. In mobile ad-hoc network every node is liberated to move severally in any direction and can so modification in it's like with different node changes often. We design our secure routing protocol based on Ad hoc On-demand Distance Vector (AODV) routing protocol. The new protocol, called TAODV (Trusted AODV) and DDAODV (Distributed Denial AODV) has several salient features: (1) Nodes perform trusted routing behaviors mainly according to the trust relationships among them; (2) A node who performs malicious behaviors will eventually be detected and denied to the whole network; (3) System performance is improved by avoiding generating and verifying digital signatures at every routing hop.

2. DDOS ATTACK

In node DDoS attacks, first the attacker physically captures the node and exploits the information on the node in a certain amount of time, reprogram the sensor node, and then place that node again inside the network. Then the attacker creates many DDoS of the captured node and places those nodes in the network. By using these nodes the attacker

can make different types of attack on the network. After compromising the node, the attacker exploits the confidential information, including secret keys and uploads it on other DDoS nodes. Other nodes in the network assume them as legitimate nodes, as they have valid credentials. So these clone nodes can communicate with the other nodes in the network.

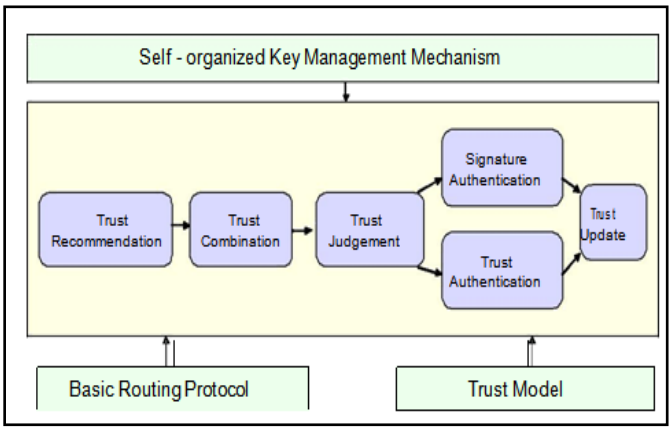

Fig 1: Framework of the Trusted AODV (TAODV)

AODV (Ad hoc On-demand Distance Vector): This routing protocol is one of the most popular routing protocols for MANETs. On-demand is a major characteristic of AODV, which means that a node only performs routing behaviours when it wants to discover or check route paths towards other nodes. This will greatly increase the efficiency of routing processes. Routing discovery and routing maintenance are two basic operations in AODV protocol.

3. CLASSIFICATION OF PROTOCOLS

Routing techniques are needed for sending information between sensor nodes and also the base stations for communication completely different routing protocols are proposed for wireless sensor network. These protocols are classified consistent with completely different parameters. Protocols will be classified as supported their mode of functioning and kind of target applications.

- **Proactive.**
- **Reactive.**
- **Hybrid**.

In a proactive protocol the nodes start their sensors and transmitters, sense the atmosphere and transmit the information to as through the predefined route. The Low Energy adaptive clustering hierarchy protocol (AODV) utilizes this kind of protocol [2].

4. PROPOSED PROTOCOL

In our work, we mainly focus on the module of trust model and trusted routing protocol. Our trusted routing protocol and trust model can be applied to different routing protocols in MANET and we will take AODV routing protocol for example to illustrate our ideas.A self-organized key management mechanism, such as threshold secret share solutions in [5] or [6], can cooperate with the TAODV. These solutions provide secure ways to issue public key certificates which can be used for the generation and verification of digital signatures during the initialization of the TAODV or a newly joined node. In these cases, certificates are issued corporately by several nodes, which is consistent with the ways of updating trust relationships in the TAODV and with our motivation of keeping any operation self-organized. Furthermore, the TAODV and the self-organized key management scheme can benefit from each other. The selection of trusted certificate issuers in key management can refer to the trust information among nodes; and the digital signature extension is a good supplement to perform trusted routing operations.

In the TAODV, we also assume that the system is equipped with some monitor mechanisms or intrusions detection units either in the network layer or the application layer so that one node can observe the behaviours of its one-hop neighbours. These mechanisms have been proposed in some previous work, such as intrusion detection system.

5. IMPLEMENTATION AND RESULTS

In this work, the random way point static model is used for the simulation of WSN routing protocols. The source-estimation pairs are spread randomly over the network where the point to point link is established between them. In this work UDP agent with CBR traffic is used with 40 packet size and 10kbps rate used for the transmission. The simulation configuration for static nodes consists of many network components and simulation parameters that are shown in the table in detail.

6. NETWORK SIMULATION

Generally network simulators try to model the real world networks. The principle idea is that if a system can be modelled, then future of the model can be changed and the

corresponding results can be analyzed. Following features are provided by simulator.

- Easy network topology setup
- Protocols and application implementation
  - UDP
  - FTP, Telnet, Web, CBR, VBR
  - Routing protocols
  - Queue management protocols
- Configurability
- Extensibility

Packet Delivery Ratio:

Packet delivery ratio is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent by sender. The fig shows the effect to the packet delivery ratio (PDR) measured for the AODV, TAODV protocols when the node Density is increased. It is measured that the packet delivery ratio.

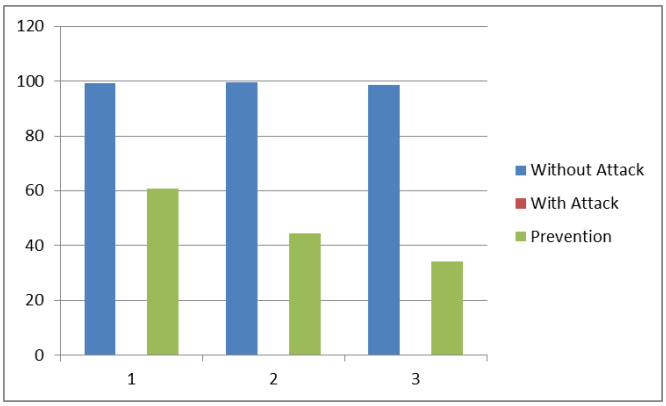

Fig 2: PDR Result

Throughput

Network throughput is the average of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second or data packets per time slot.

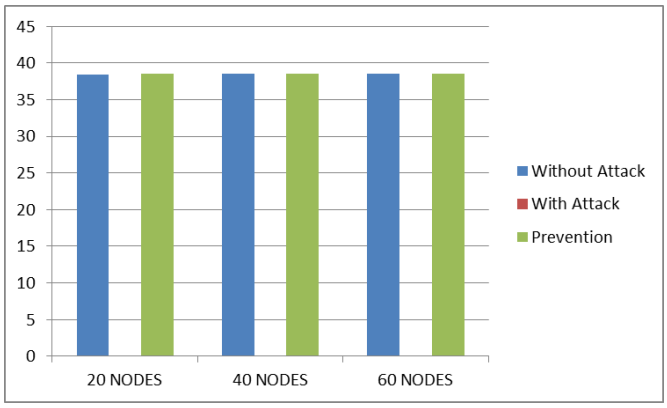

Fig 3: Throughput Result

Energy

This is the average Energy between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes.

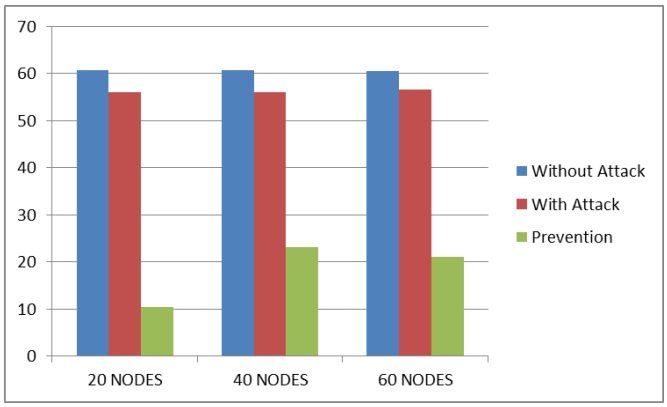

Fig 4: Energy Result

End to End Delay

This is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes.

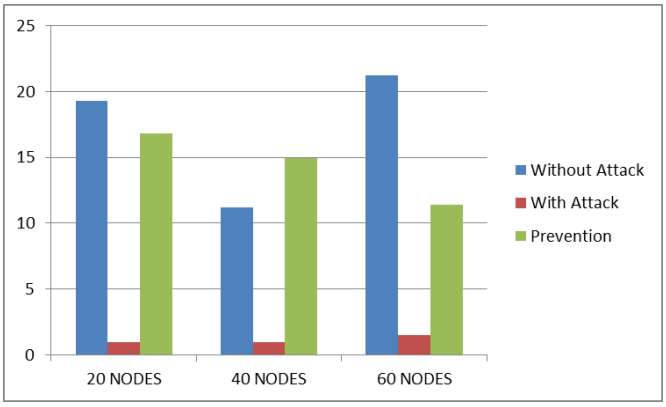

Fig 5: End To End Delay Result

Normalized Routing Load

Normalized Routing Load the number of routing packets transmitted per data packet delivered at the destination. Each hop -wise transmission of a routing packet is counted as one transmission.

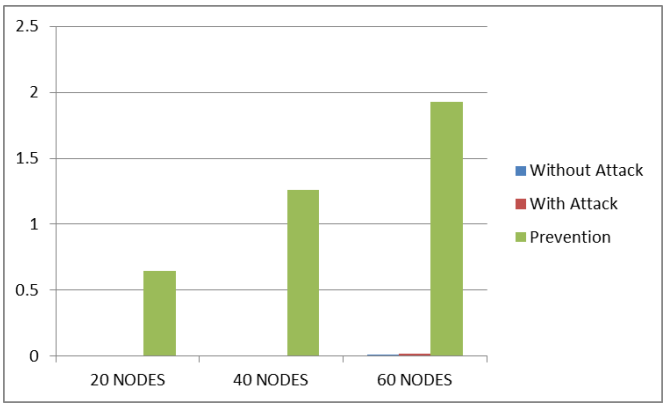

Fig 6: NRL Result

7. CONCLUSION

As the use of MANETs increases, the protection becomes may be a critical issue. During this paper, we have got mentioned the DDoS assaults in MANET and connected DDoS recognition methods. We have got also present projected defense framework against DDoS attack in MANET. It is concluded that among all network attacks, DDoS attacks are the most harmful threats to network performance metrics are analyzed for the protocols used AODV, TAODV, DDAODV, Attack, without and Prevention routing protocols by varying the node density for fixed network. Simulation of routing protocols provides. Simulation results show that, as the density of nodes increases in the network, the performance of the routing protocols decreases. Attacker nodes affect the performance of routing protocols most as path break increases. functionality and MANETs are even a lot of vulnerable to those attacks. This work carried out the detailed analysis of DDoS attack prevention and its detection through the trust mechanism with AODV routing protocol which is simulated by NS-2 for WSN on the basis of different performance metrics viz. packet delivery ratio, end to end delay, residual energy and average throughput. These According to simulation results as the Attack prevent through the Prevention, the packet delivery ratio, Throughput and End to End delay of routing protocol increases as compare to the detection of prevention through the without attack.

REFERENCES

[1] C. E. Perkins and E. M. Royer. Ad hoc on-demand distance vector routing. In Proceedingsof the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA ’99), 1999http://citeseer.nj.nec.com/article/perkins97adhoc.html.

[2] Mohsin Raza Jafri, Nadeem Javaid, Akmal Javaid, Zahoor Ali Khan, “Maximizing the Lifetime of Multi-chain PEGASIS using Sink Mobility”, Mar 18, 2013

[3] Ouadoudi Zytoune1 and Driss Aboutajdine, “A Lifetime Extension Protocol for Data Gathering in Wireless Sensor Networks” , International Journal of Innovation and Applied Studies ISSN 2028-9324 Vol. 4 No. 3 Nov. 2013, pp. 477-482

[4] Samia A. Ali and Shreen K. Refaay, “Chain-Chain Based Routing Protocol”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.

[5] S. Capkun, L. Buttyan, and J.-P. Hubaux. Self-organized public-key management for mobile ad hoc net-works. In Proceedings of ACM Workshop on Wireless Security (WiSe ’02), Atlanta, USA, September 2002. http://citeseer.nj.nec.com/capkun02selforganized.html.

[6] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. In Proceedings of IEEE ICNP ’01, 2001.

[7] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In Proceedings of the 6th ACMAnnual International Conference on Mobile Computing and Networking (MobiCom ’00), pages 275–283,Boston, Massachusetts, USA, 2000. ACM Press. http://doi.acm.org/10.1145/345910.345958.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc net-works. In Proceedings of Mobile Computing and Networking (MobiCom ’00)), pages 255–265, 2000.http://citeseer.nj.nec.com/marti00mitigating.html

[9] George Theodorakopoulos and John S. Baras, On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks. IEEE JSAC, Vol.24. No.2, February 2006.
[10] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, Elseiver publications 2003.
[11] Jie Li and Jien Kato, Future Trust Management Framework for Mobile Ad hoc Networks. IEEE Communications Magazine, April 2008.
[12] Panagiotis Papadimitratos and Zygmunt J.Haas, Secure Data Communication in Mobile Ad hoc Networks, IEEE JSAC, Vol.24, No.2, February 2006.
[13] Jonathan M. McCune, Elaine Shi, Adrian Perrig, Michael K. Reiter, "Detection of denial-of-message attacks on sensor network broadcasts", Proceedings of IEEE Symposium on Security and Privacy, May 2005.
[14] Jelena Mirkovic and Peter Reiher, D-WARD: A Source- End Defense against Flooding Denialof- Service Attacks,IEEE Transactions On Dependable And Secure Computing, Vol. 2, No. 3, 2005.
[15] Rathna. R and Sivasubramanian, ― Improving energy efficiency in wireless sensor networks through scheduling and routing‖, International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.1, January 2012.
[16] Razieh Sheikhpour, Sam Jabbehdari and Ahmad khademzadeh, ― A Cluster-Chain based Routing Protocol for Balancing Energy Consumption in Wireless Sensor Networks ‖, International Journal of Multimedia and Ubiquitous Engineering Vol. 7, No. 2, April, 2012.
[17] Se-Jung Lim and Myong-Soon Park, ― Research Article Energy-Efficient ChainFormation Algorithm for Data Gathering in Wireless Sensor Networks‖, International Journal of DistributedSensor Networks Volume 2012, Article ID 843413, 9 pages doi:10.1155/2012/843413 July 2012.