# DETECTION AND PREVENTION OF DoS ATTACK IN MANET SCENARIO USING TAODV PROTOCOL

Ramshanker Rajput[1], Megha Gupta Jat[2], Avinash Pal[3]
Department of Information Technology, Patel College of Science & Technology, Indore[1,2, 3]

***Abstract:*** *In this paper, we design and formulate a IDS-based routing protocol to secure nodes from attack i.e. Denial-of service attack, in mobile ad hoc networks (MANETs). The innovative approach is employing the idea of a secure 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 DoS attack. DoS attack has the flexibility to make immense quantities of unwanted traffic as a result of this the licensed user cannot use the resources properly. It is terribly laborious to notice and manage the DoS attack as a result of massive scale and complicated network environments. The scope of this paper is to study the effects of DoS attack in Ad hoc On-demand Distance Vector (AODV) [1] routing protocol. The new protocol, called TAODV is implemented by enhancing traditional AODV protocol. Comparative analysis of DoS attack for both protocols is taken into account. The impact of Node DoS attack on the performance of MANET is evaluated by finding out which protocol is more exposed to the attack and how much are the contacts 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, DoS attack, AODV, and TAODV Routing Protocols, NS-2.35.*

## 1. INTRODUCTION

A mobile ad hoc network (MANET) [10][12] is a kind of wireless network without centralized administration or fixed network infrastructure, in which nodes communicate over relatively bandwidth constrained wireless links and perform routing discovery and routing maintenance in a self- organized way. The topology of the MANET may change uncertainty and rapidly due to the high mobility of the independent mobile nodes, and because of the network decentralization, each node in the MANET will act as a router to discover the topology and maintain the network connectivity. Unlike the wired networks, the MANET must take into account many factors such as wireless link quality, power limitation, and multiuser interference and so on. The routing determination is also more difficult in the MANET. Nowadays the MANET enables many promising applications in the areas of emergency operations, disaster relief efforts, and military battlefield networks.

Many security schemes from different aspects of MANETs have been proposed in recent years, such as secure routing protocols [17] and secure key management solutions [9], [13], [14], [16]. However, most of them assume centralized units or trusted third-parties to issue digital certificates, which actually destroy the self-organization nature of MANETs. And by requiring nodes to perform digital signature authentication all the time, these solutions often bring huge computation overheads. Our solution is, on the other hand, a secure routing protocol which employs the idea of IDS so that it can avoid introducing large overheads and influencing the self-organization nature of MANETs.

We develop a technique to identify denial of service nodes. The technique works with slightly changed AODV protocol to offer the strategy of preventing denial of service attack by using IDS algorithm. We propose a solution that's an improvement of the fundamental AODV routing protocol, which can be capable of avoiding denial of services to reduce the probability of denial of service, it's proposed IDS based mostly methodology for forestall denial of service and realize a safe route to achieve the neighboring nodes. A wireless IDS monitors wireless network traffic and analyses its wireless networking Protocol to identify suspicious activity.

In mobile ad-hoc networks every node is liberated to move severally in any direction and can so modify it 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 DAODV (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. THE DENIAL OF SERVICE PROBLEM IN CURRENT AODV PROTOCOL

Denial of service attack in MANETS may be a serious security problem to be solved. During this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it desires to intercept. AODV is a vital on-demand routing protocol that makes routes only desired by the source node. Once a node needs a route to a destination, it initiates a route discovery process within the network. It broadcasts a route request (RREQ) packet (Fig. 2.1) to its neighbors, that then forwards the request to their neighbors, and so on, till either the destination or AN intermediate node with a "fresh enough" route to the destination is found. During this process the intermediate node will reply to the RREQ packet only if it's a fresh enough route to the destination. Once the RREQ reaches the destination or AN intermediate node with a recent enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from that it 1st received the RREQ. Once choosing and establishing a route, it's maintained by a route maintenance procedure till either the destination becomes inaccessible along each path from the source or the route isn't any longer desired.

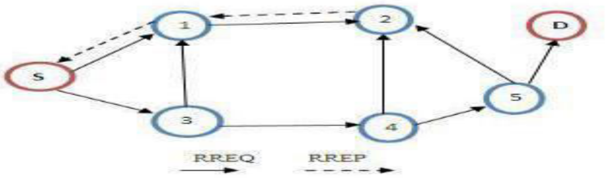

**Figure: 2.1 Broadcasts a route request (RREQ) packet**

During this article we address one routing attack that might simply happen in wireless MANETs, the denial of service problem. According to the initial AODV protocol, any intermediate node could reply to the RREQ message if it's a fresh enough route that is checked by the destination sequence number contained within the RREQ packet. This mechanism is used to decrease the routing delay, but it makes the system a target of a malicious node. The malicious node simply disrupts the correct functioning of the routing protocol and makes at least a part of the network crash. As an example Node one desires to send data packets to node four in Fig. 2.2, and initiates the route discovery process. We have a tendency to assume node three to be a malicious node with no fresh enough route to destination node four. However, node three claims that it's the route to the destination whenever it receives RREQ packets, and sends the response to source node one. The destination node and the other normal intermediate nodes that have the fresh route to the destination can also give a reply. If the reply from a normal node reaches the source node of the RREQ 1st, everything works well; however, the reply from malicious node three may reach the source node 1st, if the malicious node is nearer to the source node. Moreover, a malicious node doesn't need to check its routing table once sending a false message; its response is a lot of possible to reach the source node 1st. This makes the source node assume that the route discovery process is complete, ignore all different other reply messages, and start to send data packets. As a result, all the packets through the malicious node are simply consumed or lost. The malicious node can be said to form a denial of service within the network, and that we call this the denial of service problem. During this way the malicious node will simply misroute lots of network traffic to itself, and will cause an attack to the network with very little efforts on its part.

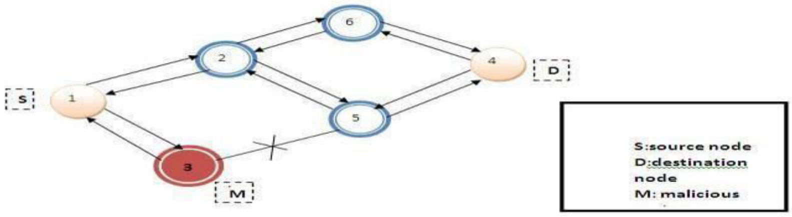

**Figure: 1.2 Denial of Service Problem**

## 3. PROPOSED PROTOCOL

Mobile Ad-hoc Network consists of some nodes that are standing randomly in an operational environment without any predefined infrastructure and mobility which are vulnerable for intrusion and attack. Security is an important field in this type of network. Use IDS (intrusion detection system) based approach to detect and prevent denial of service in MANET. IDS detect and report the malicious activity in ad hoc network. Intrusion detection systems (IDSs) do just that: monitor audit data, look for intrusions to the system, and initiate a proper response.

This work proposes a solution based on trust detection to detect attacks on AODV. This approach specifies the correct AODV routing behavior and is distributed in the network. Trust Mechanism monitors networks for detecting run-time violation of the specifications. Aim of Trust Mechanism is to secure the AODV protocol. Dynamic topologies make it difficult to obtain a global view of the network. Traffic monitoring in wired networks is usually performed at switches, routers and gateways, but an Ad Hoc network does not have these types of network elements so here Trust Mechanism can collect audit data for the entire network. Trust Value is defined as a sequence of related actions performed by a malicious adversary that results in the compromise of a target network. The existence of a security policy that states which actions are considered malicious should be prevented is a key requisite for an intrusion detection system to work. Trust detection is the process of identifying and responding to malicious activities targeted at computing and network resources.

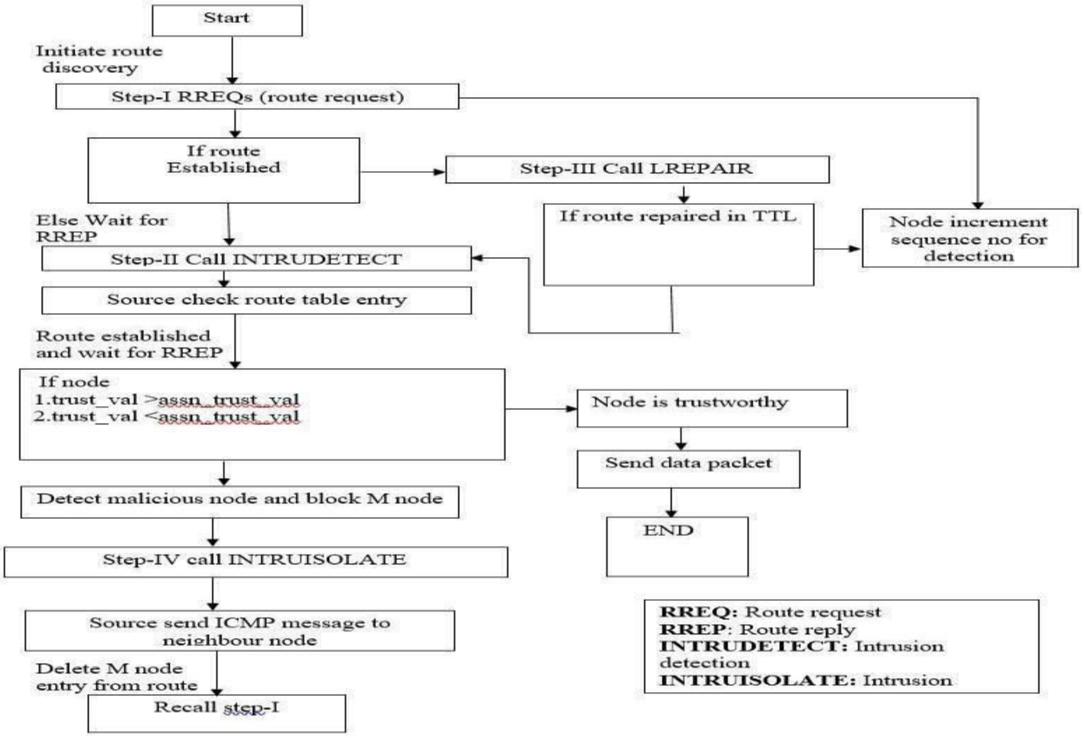
Start
Initiate route discovery
Step-I RREQs (route request)
If route Established
Step-III Call LREPAIR
Else Wait for RREP
If route repaired in TTL
Node increment sequence no for detection
Step-II Call INTRUDETECT
Source check route table entry
Route established and wait for RREP
If node
1.trust_val >assn_trust_val
2.trust_val <assn_trust_val
Node is trustworthy
Send data packet
END
Detect malicious node and block M node
Step-IV call INTRUISOLATE
Source send ICMP message to neighbour node
Delete M node entry from route
Recall step-I
RREQ: Route request
RREP: Route reply
INTRUDETECT: Intrusion detection
INTRUISOLATE: Intrusion

**Figure: 3.1 Flow Chart of TAODV Protocol**

## 4. NETWORK SIMULATION

Generally network simulators try to model the real world networks. The principle idea is that if a system can be modelled, then the future of the model can be changed and the corresponding results can be analyzed. Following features are provided by the simulator.

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

**Table 4.1 Simulation Parameters**

| | |
|---|---|
| Simulation tool | Network simulator-2.35 |
| IEEE scenario | MANET(802.11) |
| Mobility model | Two ray ground |
| Number of nodes | 20,40,60 |
| Node movement speed | 10m/sec,28m/sec. |
| Traffic type | UDP |
| Antenna | Omni Directional Antenna |
| MAC Layer | IEEE 802.11 |
| Routing Protocol | AODV, DAODV, TAODV |
| Queue limit | 50 packet |
| Simulation area(in meter) | 1000*1000 |
| Queue type | Drop-tail |
| Channel | Wireless channel |

## 5. IMPLEMENTATION AND RESULTS

In this work, the random waypoint mobility model is used for the simulation of MANET routing protocols. The source-destination 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 mobile nodes consists of many network components and simulation parameters that are shown in the table in detail. Generally, network simulators try to model the real world networks. The principle idea is that if a system can be modelled, then futures of the model can be changed and the corresponding results can be analyzed.

- **PACKET DELIVERY RATIO**

This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes. Figure and table shows the Packet delivery ratio under Denial of service attack detection and its prevention through Trust based mechanism i.e. AODV, DAODV and TAODV for the various node density.

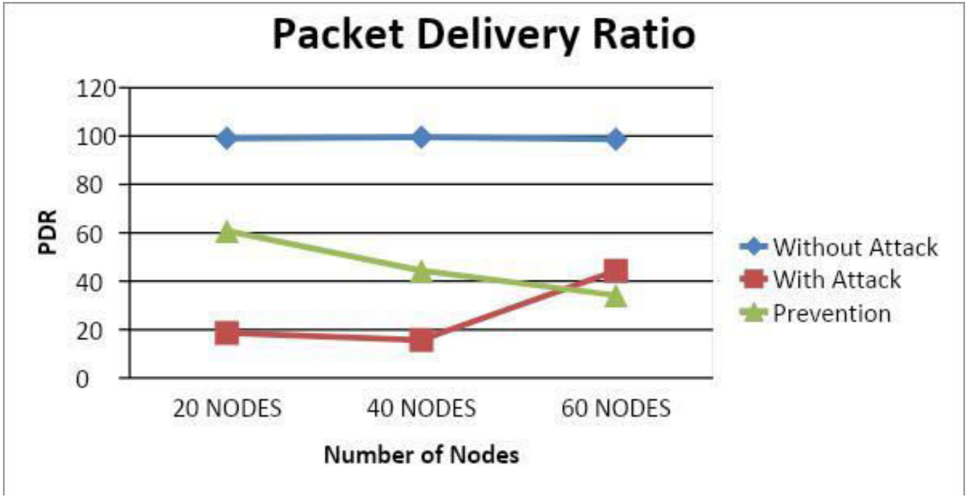

Figure: 5.1 Packet Delivery Ratios

| No of Nodes | Attack | Prevention | Without |
|---|---|---|---|
| 20 | 18.6 | 60.77 | 99.08 |
| 40 | 15.7 | 44.32 | 99.57 |
| 60 | 44.32 | 34.16 | 98.71 |

Table: 5.1 Packet Delivery Ratios

- **THROUGHPUT**

This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes. Figure and table shows the Throughput under Denial of service attack detection and its prevention through Trust based mechanism i.e. AODV, DAODV and TAODV for the various node density.

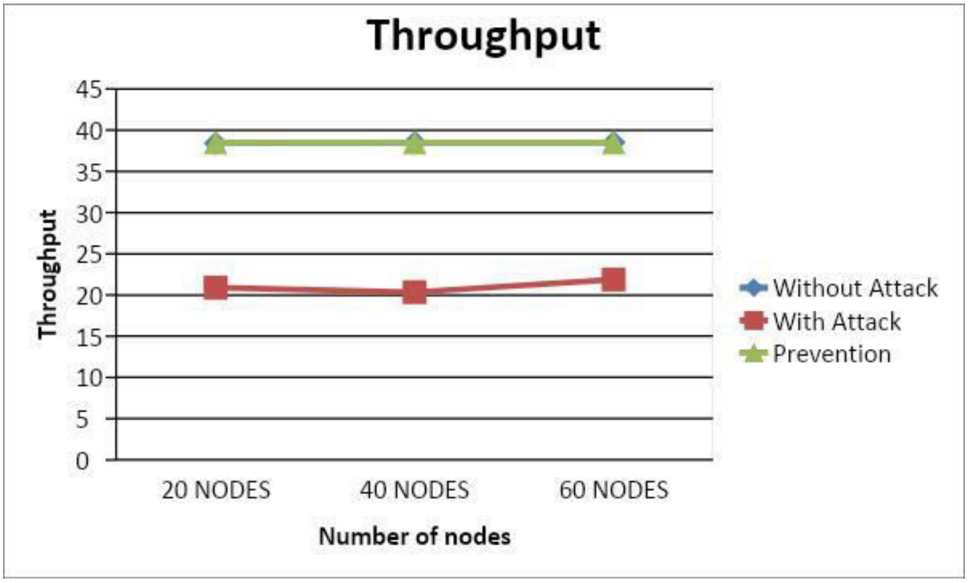

Figure: 5.2 Throughputs

Table: 5.2 Throughputs

| No. of Nodes | Attack | Prevention | Without |
|---|---|---|---|
| 20 | 20.9 | 38.50 | 38.41 |
| 40 | 20.34 | 38.50 | 38.50 |
| 60 | 21.87 | 38.50 | 38.50 |

- **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. Figure and table shows the End to End Delay under Denial of service attack detection and its prevention through Trust based mechanism i.e. AODV, DAODV and TAODV for the various node density.

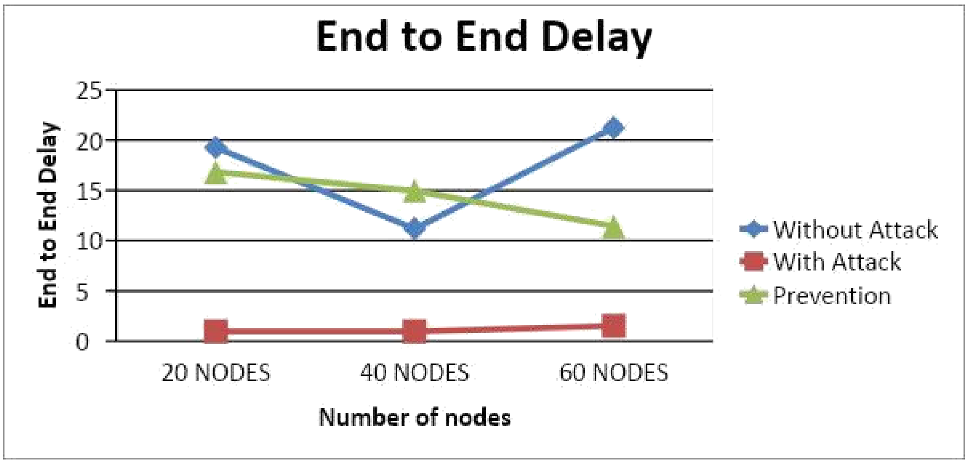

Figure: 5.3 End to End Delays

Table: 5.3 End to End Delays

| No of Nodes | Attack | Prevention | Without |
|---|---|---|---|
| 20 | 0.969396 | 16.7985 | 19.2717 |
| 40 | 0.9697 | 14.9544 | 11.1819 |
| 60 | 1.50503 | 11.4302 | 21.2035 |

- **RESIDUAL ENERGY**

It is the total amount of remaining energy by the nodes after the completion of Communication or simulation. If a node is having 100% energy initially and having 70% energy after the simulation then the energy consumption by that node is 30%. The unit will be in Joules. Figure and table shows the Residual Energy under Denial of service attack detection and its prevention through Trust based mechanism i.e. AODV, DAODV and TAODV for the various node density.

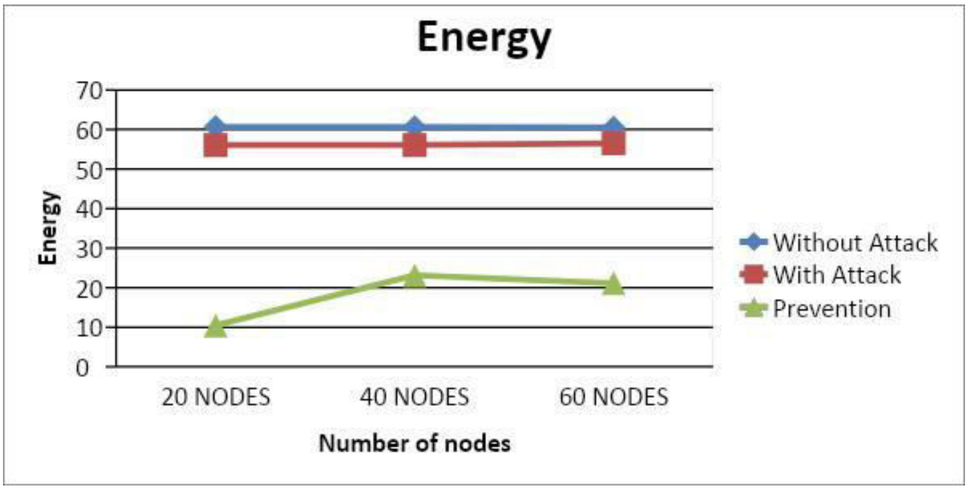

Figure: 5.4 Residual Energy

Table: 5.4 Residual Energy

| No of Nodes | Attack | Prevention | Without |
|---|---|---|---|
| 20 | 56.06 | 10.45 | 60.64 |
| 40 | 56.06 | 23.12 | 60.61 |
| 60 | 56.51 | 21.13 | 60.53 |

## 6. CONCLUSION

As the use of MANETs increases, the protection becomes may be a critical issue. During this paper, we have got mentioned the DoS assaults in MANET and connected DoS recognition methods. We have got also present projected defense framework against DoS attack in MANET. It is concluded that among all network attacks, DoS attacks are the most harmful threats to network performance metrics are analyzed for the Protocols used AODV, TAODV, DAODV, 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 DoS 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. We found that there is 70-75% PDR for Secure TAODV. This clearly shows that there is a significant benefit when the solution against Denial of service attacks is applied. There was 70%-80% Throughput in Secure TAODV under Denial of service Attack, which indicates solution work better even though number of nodes increases. However, there is a 30-40% decrease in Residual Energy for Secure TAODV compared to normal AODV as TAODV consume more energy in preventing network from Dos attack. There is a 10-20% decrease in End-to-End Delayfor Secure TAODV compared to normal AODV.

## REFERENCES

[1] Raksha Upadhyay, Salman Khan, Harendra Tripathi and Uma Rathore Bhatt, ”Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain”, Intl. Conference on Computing and Network Communications (CoCoNet’15), Dec. 16-19, 2015

[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 Zyt oune1 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 hocnet-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 ACM Annual 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 ofMobile 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] ImrichChlamtac, 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] PanagiotisPapadimitratos and ZygmuntJ.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] JelenaMirkovic 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] RaziehSheikhpour, 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 Chain Formation Algorithm for Data Gathering in Wireless Sensor Networks ‖, International Journal of Distributed Sensor Networks Volume 2012, Article ID 843413, 9 pages doi:10.1155/2012/843413 July 2012.

[18] Bhavin Joshi and Nikhil Kumar Singh, “Mitigating Dynamic Dos Attacks in Mobile Ad Hoc Network”, Symposium on Colossal Data Analysis and Networking (CDAN), IEEE 2016.