ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Performance of Improved Trust Based Mobile Ad-hoc Network Routing Protocol for MANET

Shiv Kumar Dwivedi [1], Mohammed Bakhtwar Ahmed [2]

P.G. Student, Department of Computer Engineering, Kalinga University, Raipur, India[1]

Assistant Professor, Department of Computer Engineering, Kalinga University, Raipur, India[2]

ABSTRACT: Mobile Ad Hoc Network (MANET) is collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure. The wireless links in this network are highly error prone and can go down frequently due to mobility of nodes, interference and less infrastructure. Therefore, routing in MANET is a critical task due to highly dynamic environment. The nodes of mobile ad hoc networks are susceptible to compromise. In such a scenario, designing an efficient, trustworthy and secure routing protocol has been a major challenge over the last many years. They are characterized by the use of wireless links, dynamically changing topology, multi-hop connectivity and decentralized routing mechanism and decision making. The performance of Ad-hoc On Demand Vector (AODV) protocols has been modified by including the source route accumulation feature. As low transmission power of each ad-hoc node limits its communication range, the nodes must assist and trust each other in forwarding packets from one node to another. There are many attacks in MANET due to which the legitimacy of a network is compromised such as, Black Hole Attack, Worm Hole Attack, Byzantine attack, DoS attack. So, secure communication in MANET is essential and challenging task. In this paper, we present "Improved Trust Based Mobile Ad hoc Network Routing Protocol for MANET". Our proposed algorithm works on the concept of honest value which is calculated on the concept of hop and trust to protect the network from malicious node. The performance of the proposed protocol is analyzed using throughput, number of drop packets, packet delivery ratio and number of received packets with the variation of number of nodes, speed and simulation time. Results show that the proposed method has better performance and enhance the security in the network.

KEYWORDS: Trust, honest values, security, attacks, AODV, Security, Trusted AODV, MANET.

I. INTRODUCTION

MANET Stands for "Mobile Ad Hoc Network." A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard wi-fi connection, or another medium, such as a cellular or satellite transmission. Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network.

Generation of mobile ad-hoc network

In first generation they were used for different military scenarios. A packet radio network was the first ad-hoc network system.

In second generation from 1980s' to the mid 1990's. It's main aim were the same as for the first generation ad-hoc networks system i.e. aiding combat operations. Second generation developments focused on the further advancement of the previously build ad-hoc network structure. Some important developments; Global Mobile Information Systems, Near Term Digital Radio (NTDR).

In third generation ad-hoc network systems are also known as commercial ad-hoc network systems. These developments, Bluetooth – ad-hoc sensor networks etc.

Types of MANET

There are following types of MANET as described as:

a) VANETs
b) SPANs
c) iMANETs
d) Military / Tactical MANETs

VANETs:

It stands as Vehicular Ad hoc Networks are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (In VANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents.

SPANs:

It stands as Smart Phone Ad hoc Networks are leverage the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smart phones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. SPANs differ from traditional hub and spoke networks, such as Wi-Fi Direct, in that they support multi-hop relays and there is no notion of a group leader so peers can join and leave at will without destroying the networks.

iMANETs:

It stands as Internet based mobile ad hoc networks are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. For example, multiple sub-MANETs may be connected in a classic Hub-Spoke VPN to create a geographically distributed MANET. In such type of networks normal ad hoc routing algorithms don't apply directly. One implementation of this is Persistent System's Cloud Relay.

Military / Tactical MANETs:

These are used by military units with emphasis on security, range, and integration with existing systems. Common waveforms include the US Army's SRW, Harris's ANW2 and HNW, Persistent Systems' Wave Relay, Trellis ware's TSM and Silvus Technologies' Stream Caster.

Architecture of MANET

The specific MANET issues and constraints described above pose significant challenges in ad-hoc network design. To present the huge amount of research activities on ad hoc networks in a systematic/organic way, we will use, as a reference, the simplified architecture shown in Fig.1.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

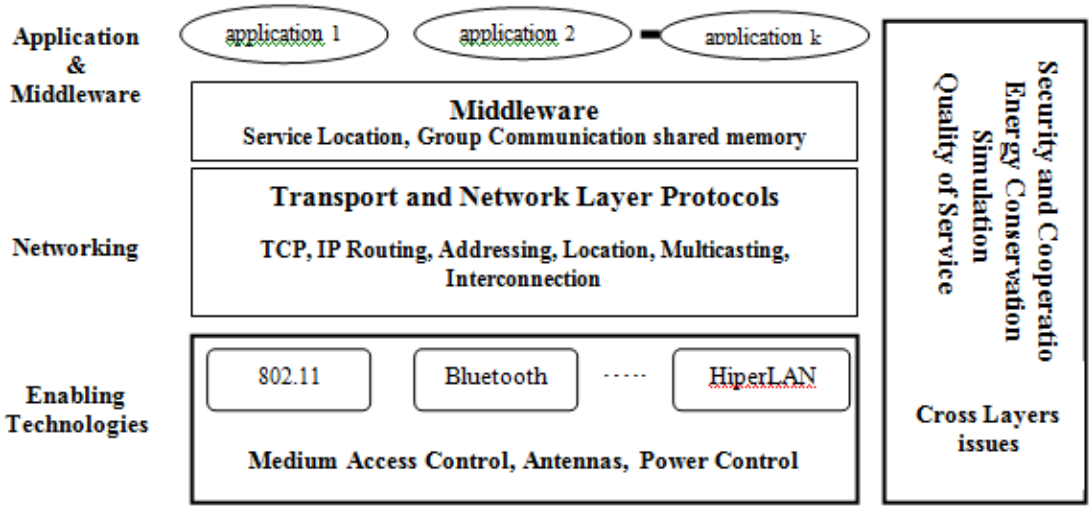

Fig. 1. A Simple MANET Architecture.

Ad-hoc On-Demand Distance Vector Routing (AODV)

AODV is a reactive routing protocol. When a node requires a route, it initiates a route discovery procedure broadcasting Route Request (RREQ) messages. When a node receives a RREQ, if either it has a valid route entry to the demanded destination or it is the destination itself, it creates and sends a Route Reply (RREP) message back to the originator node. Every node maintains route entries with forward and backward next hop information that expire after a specified time if the path becomes inactive (i.e., it is not used for data transmission). For each route entry of a node, there exists a predecessor list containing the nodes that use this one as the next hop in the path to a given destination. The metric used in AODV is the hop count. Loop-freedom of routes towards a destination is guaranteed by means of a destination sequence number, which is updated whenever new information about that destination is received. When a link breaks along an active path, the upstream node that detects this break may locally repair the route if the destination is close in number of hops to the node. If local repair cannot be completed successfully or the option is not supported, the node that detects the link break creates a Route Error (RERR) message which reports the set of destinations that are now unreachable and sends it to predecessor nodes. Then, the source of the active path starts a new route discovery phase if a route to the destination is still needed. Data packets waiting for a route should be buffered during route discovery.

Dynamic source routing (DSR)

In the Dynamic Source Routing (DSR) protocol for ad hoc networks, due to the rapidly changing network topology, a route discovery is used to dynamically discover a route to any other node in the network in an “on demand” manner. This is achieved by the source broadcasting a route request packet specifying the intended destination. On reception of a route request by a node that is not the intended destination, if this node has not already processed this packet before, it will append its identifier onto the route in the packet header and re-broadcast the packet. If the receiver of the route request packet is the intended destination, then it returns a route reply packet to the initiator of the route discovery, following the newly constructed path in the reverse order. Once the source route is computed, the packet is processed in a method similar to any source routing protocol.

II. PROBLEM IDENTIFICATION

As per our knowledge, there is no solution has been proposed so far to secure the network against internal attack using such mechanism which is combination of hop value and trust value. Here, we present the related work done by various researchers on trust based scheme for mobile ad hoc network, which extended Ad Hoc On-demand Distance Vector (AODV) routing protocol. AODV is an on demand routing protocol which comes under the category of reactive routing

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

protocol. Route discovery and route maintenance are the two basic operation of AODV. Route discovery operation is used to discover the route by using RREQ (route request) and RREP (route reply) control message. When a source node wants to send the data to destination node, it will broadcast RREQ packet to neighbours and then to their neighbours & so on. When a destination node receives RREQ, it will send RREP to source node. In this paper existing work has been discussed about an trust based ad hoc on demand routing protocol for MANET called HAODV (honest ad hoc on demand distance vector routing protocol) where honest value will be initialized (one value will be based on the hop and other will be based on the trust) in the initialization phase. Security issues in MANET have drawn considerable attention over past few years. Using trust to improve the security is an active area of research. As per my knowledge the following problems are identified:

- There is no solution has been proposed so far to secure the network against internal attack using such mechanism which is combination of hop value and trust value.
- Network is depending on trust value and based on single methodology (used single routing factor).

III. RELATED WORK

In the based paper, Trust Based Ad-hoc On Demand Routing Protocol for MANET is presented honest based general framework for trust establishment and management in the network using AODV routing protocol. We proposed a best trust-based scheme for securing AODV routing protocol in MANET using the honest mechanism. In the honest mechanism, two honest value will be initialized (one will be based on the hop and other will be based on the trust). The honest value based on the hop will be incremented and decremented during RREQ and RREP phase respectively and the honest value based on trust value will be used for trust calculation of path. In the proposed HAODV routing protocol, the nodes can evaluate the routing paths according to our trusted metrics before forwarding the data through these routes. For identity information we will use password value. This scheme is believed to provide a robust environment where MANET nodes can trust each other in a secure community.
We are including new trust based network routing factors as follows:
a) Distance- which is based on Physical Distance.
b) Degree-which is based on Connection.

For solving these routing factors the following algorithm is described as follows:

1) Node creation and authentication.

- Create a simple pair of nodes and start communication between the two nodes.
- Assume that each node has identity information that cannot be forged by malicious nodes. This Identity information can be some type of smart card provided in the initialization phase. For simplicity, we use IP and MAC addresses.
- Assume that the number of malicious nodes is less than the number of good nodes.

2) Honest value initialization (Based on the Hop and Based on the Trust)
The initialization phase or when the node will configure every node will have two values that are honest values (one will be based on the hop and other will be based on the trust).

- Based on the hop the values will be evaluated for each node using the following equation

M = P * Q
Where,
M = Current value of every node
P = Total number of hops from source to destination
Q = Number of hops from source to the current node

- Based on the trust the values are calculated using the following equation

N = Constant number * Q

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Where, N= Current trust value of every node.

3) Communication and path evaluation

In the route discovery phase when the route is needed, the source sends the RREQ packet in a controlled flooding manner throughout the network, any node in the network which receives the RREQ packet can answer with a RREP.

RREQ -

When RREQ packet will go from source node then the honest value based on the hop at each node will decrease by one and honest value based on the trust will remain same in the RREQ phase.

RREP –

When RREP packet will come from destination to source first every node will check in its routing table that neighbor node is in the list or not, if neighbor node is in the list then only it will send the RREP packet.

Then it will calculate the path value and compare it with the existing route path value if the calculated value is more, then it will register that path and forward the RREP packet with that route.

In the RREP phase it will calculate the honest or trust value based on the hop with summation of RREP value (Earlier it has depend on honest value based on the hop or single route) for every node. The following formula can be used to evaluate the trusted and shortest path.

$$SP = \frac{\text{Sum of trust values} * \sqrt{\text{No of hopes}}}{\text{No of hops}}$$

Where,

Sum of trust value = $\sum$ trustvalue (i)

SP = Shortest Path, trustvalue(i) = Trust value of i node

IV. CONCLUSION & FUTURE WORK

A method based on the honest method to protect the AODV routing protocol has been accessible. The performance of HAODV has been analyzed via the four parameters i.e. the number of dropped packets, Throughput, Overhead Routing and Packet delivery ratio. The based paper's simulation results show that HAODV performs well in terms of throughput and no of dropped packets but in terms of PDR, AODV is better. The throughput of HAODV is always improved as compared to AODV even by increasing the number of nodes, by unreliable the velocity, etc. In HAODV least number of packets is dropped in comparison to AODV. Honest based routing protocol proved to be best in terms of packet loss, throughput and power consumed. The packets will delivers from source node to destination node through a multiple node but reached by shortest distance of route except all other routes.

The future work of this research is to implement the proposed scheme with more numbers of parameters as like End to End Delay and Overhead Routing while evaluating the path. Our future work is to be minimizing the dropped packets with a single node, show the reason why packets are dropped and find out which nodes will drop packets. It will also choose a best path and shortest path for requesting packets to send from source to destination at a time except on single path.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

REFERENCES

[01]Tameem Eissa & Shukor Abdul Razak & Rashid Hafeez Khokhar & Normalia Samian, "Trust-Based Routing Mechanism in MANET: Design and Implementation", Springer Science, 2011.
[02]Akshai Aggrawal, Savita Gandhi, Nirbhay Chaubey & Keyurbhai A. Jani, "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs", 2014.
[03]Watchara Saetang and Sakuna Charoenpanyasak ,"CAODV: Free Blackhole Attack in Ad Hoc Networks", International Conference on Computer Networks and Communication Systems, IPCSIT vol-35, 2012.
[04]Dr.S.S.Dhenakaran & A.Parvathavarthini, "An Overview of Routing Protocols in Mobile Ad-Hoc Network, IJARCS,2013.
[05]R.Balakrishna, U.Rajeswar Rao , G.A.Ramachandra , M.S.Bhagyashekar, Trust-based Routing Security in MANETS, IJCSE, 2010.
[06]Yogendra Kumar Jain, Pankaj Sharma "Trust based Ad hoc On-demand Distance Vector for MANET" National Conference on Security Issues in Network Technologies (NCSI-2012).
[07]Gurpinder Singh, Asst. Prof. Jaswinder Singh, MANET: Issues and Behavior Analysis of Routing Protocols, IJARCS, 2012.
[08]Krishna Gorantala, Routing Protocols in Mobile Ad-hoc Networks Ume°a University, UME°A, SWEDEN,2006.
[09]C. Gomez, P. Salvatella, O. Alonso, J. Paradells, Adapting AODV for IEEE 802.15.4 Mesh Sensor Networks: Theoretical Discussion and Performance Evaluation in a Real Environment, Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks.
[10]Vivek Arya and Charu, A SURVEY OF ENHANCED ROUTING PROTOCOLS FOR MANETs, International Journal on AdHoc Networking Systems (IJANS) Vol. 3, No. 3, July 2013.
[11]Mohamed Amnai, Youssef Fakhri, Jaafar Abouchabaka, Impact of Mobility on Delay-Throughput Performance in Multi-Service Mobile Ad-Hoc Networks, Int'l J. of Communications, Network and System Sciences, 2011, 4, 395-402.
[12]Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, Mobile ad hoc Networking: imperatives and challenges, Chapter in Ad Hoc Networks, Page 13-64, 2003.
[13]Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen, " A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, 2011.
[14]NaghamH. Saeed, MaysamF. Abbod, and Hamed S. Al- Raweshidy ," MANET Routing Protocols Taxonomy", International Conference on Future Communication Networks 2012.
[15]Manel Guerrero Zapata ," Secure Ad hoc On-Demand Distance Vector Routing", Mobile Computing and Communications Review, Volume 6, Number 3, 2006.
[16]S.A.Razak, S.M.Furnell,P.J.Brooke ,"Attack against Mobile Ad Hoc Networks Routing Protocols", Network Research Group ,University of Plymouth, 2009.
[17]C. E. Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Wksp. Mobile Computer Systems and Applications, 1999.
[18]Poonam Gera, Kumkum Garg, Manoj Misra ," Trust Based Multi-Path Routing for End to End Secure Data Delivery in MANETs", ACM 978-1-4503-0234-0/10/09, 2010.
[19]Naveen Kumar Gupta and Kavita Pandey, Trust Based Ad-hoc On Demand Routing Protocol for MANET, 2013.
[01]Tameem Eissa & Shukor Abdul Razak & Rashid Hafeez Khokhar & Normalia Samian, "Trust-Based Routing Mechanism in MANET: Design and Implementation", Springer Science, 2011.
[02]Akshai Aggrawal, Savita Gandhi, Nirbhay Chaubey & Keyurbhai A. Jani, "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs", 2014.
[03]Watchara Saetang and Sakuna Charoenpanyasak ,"CAODV: Free Blackhole Attack in Ad Hoc Networks", International Conference on Computer Networks and Communication Systems, IPCSIT vol-35, 2012.
[04]Dr.S.S.Dhenakaran & A.Parvathavarthini, "An Overview of Routing Protocols in Mobile Ad-Hoc Network, IJARCS,2013.
[05]R.Balakrishna, U.Rajeswar Rao , G.A.Ramachandra , M.S.Bhagyashekar, Trust-based Routing Security in MANETS, IJCSE, 2010.
[06]Yogendra Kumar Jain, Pankaj Sharma "Trust based Ad hoc On-demand Distance Vector for MANET" National Conference on Security Issues in Network Technologies (NCSI-2012).
[07]Gurpinder Singh, Asst. Prof. Jaswinder Singh, MANET: Issues and Behavior Analysis of Routing Protocols, IJARCS, 2012.
[08]Krishna Gorantala, Routing Protocols in Mobile Ad-hoc Networks Ume°a University, UME°A, SWEDEN,2006.
[09]C. Gomez, P. Salvatella, O. Alonso, J. Paradells, Adapting AODV for IEEE 802.15.4 Mesh Sensor Networks: Theoretical Discussion and Performance Evaluation in a Real Environment, Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks.
[10]Vivek Arya and Charu, A SURVEY OF ENHANCED ROUTING PROTOCOLS FOR MANETs, International Journal on AdHoc Networking Systems (IJANS) Vol. 3, No. 3, July 2013.
[11]Mohamed Amnai, Youssef Fakhri, Jaafar Abouchabaka, Impact of Mobility on Delay-Throughput Performance in Multi-Service Mobile Ad-Hoc Networks, Int'l J. of Communications, Network and System Sciences, 2011, 4, 395-402.
[12]Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, Mobile ad hoc Networking: imperatives and challenges, Chapter in Ad Hoc Networks, Page 13-64, 2003.
[13]Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen, " A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, 2011.
[14]NaghamH. Saeed, MaysamF. Abbod, and Hamed S. Al- Raweshidy ," MANET Routing Protocols Taxonomy", International Conference on Future Communication Networks 2012.
[15]Manel Guerrero Zapata ," Secure Ad hoc On-Demand Distance Vector Routing", Mobile Computing and Communications Review, Volume 6, Number 3, 2006.
[16]S.A.Razak, S.M.Furnell,P.J.Brooke ,"Attack against Mobile Ad Hoc Networks Routing Protocols", Network Research Group ,University of Plymouth, 2009.
[17]C. E. Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Wksp. Mobile Computer Systems and Applications, 1999.
[18]Poonam Gera, Kumkum Garg, Manoj Misra ," Trust Based Multi-Path Routing for End to End Secure Data Delivery in MANETs", ACM 978-1-4503-0234-0/10/09, 2010.
[19]Naveen Kumar Gupta and Kavita Pandey, Trust Based Ad-hoc On Demand Routing Protocol for MANET, 2013.