SYNOPSIS

Enrollment Number: 129990907006 Batch: 2012

Branch Name: Computer Engineering

Name of Research Scholar: Patel Kajal Shambhubhai

I. Title of the thesis and abstract

Title of Thesis

Reliable Routing Protocol for Mobile Ad Hoc Network

ABSTRACT

Mobile Adhoc NETworks (MANET) help us in setting up a network of mobile nodes like laptop, smart phones, tablet etc. without the need of any infrastructure. We can develop a temporary network in the battle field, forest, hilly area, meeting rooms, disaster area etc. whenever the need arises. There is no need of any Access Point (AP) or Base Station (BS) to build MANET. The nodes in this network can move freely and change their position and thus the topology of the network at any time. Nodes are battery operated and resource constrained. MANET uses wireless media for data communication. There is no specialized router used in MANET. Each and every node has to act as a router to forward data from source node to a destination node. The routing protocols used for wired network cannot be used for MANET due to the aforementioned characteristics of it. The routing protocols like DSDV, AODV, OLSR, DSR, etc. designed for MANET consider only dynamically changing network topology. These basic routing protocols do not consider any security issue while routing. Thus MANET is vulnerable to many security attacks as nodes uses wireless media and has to depend on unknown intermediate nodes for routing their packets. The attacks like packet drop, intentional packet delay before forwarding, eavesdropping, DoS attacks, packet modification, fabrication and replication of packets etc. can be done by intermediate nodes. These attacks may compromise confidentiality and disturb the network operation which may lead to a failure of the whole network. Apart from the aforementioned hard security threats, the MANET is also vulnerable to soft security threats like low quality of service, wrong information delivery or advertisement and malicious/malfunction activities. These soft threats are associated with behaviour of the intermediate nodes. Since the nature of the system is open, such behaviours are difficult to control. Hence, such soft threats are also difficult to detect.

To detect/avoid attacker nodes many researchers have come up with routing protocols which use various cryptographic approaches. The cryptographic approaches are very complex and have huge computational overhead on node, which is not suitable for resource constraint mobile nodes. Additionally cryptography based solutions are binary solutions. The nodes either pass or fail the security checks. In a MANET, behaviour of a node changes continuously. These changes may occur due to malicious behaviour of the nodes/hardware failure/mobility of the node. The cryptographic approaches cannot detect

such continuously changing behaviour of nodes. To solve the problem, researchers come up with a trust based routing solution. For measuring reliability, we can use the trust value associated with each node. On almost all existing trust based routing schemes, communication parameters like number of successful sessions, packet forwarded between two nodes, number of packets dropped or delayed, response time, battery life, mobility of node etc. are used for calculating trust value of a node. Researchers also use various methods for aggregating these parameters to calculate trust values like a weighted sum model, Bayesian model, fuzzy model, Markov chain based model, etc. Most of existing trust based routing protocols create a route based on trust of nodes and gives only one trustworthy route. If this route breaks, we need to reestablish other route which may add overhead. Also, all existing trust based routing protocols used most trusted nodes while the route is established. This may add extra burden to trustworthy nodes only and free other nodes from routing. Hence trustworthy nodes may overburden in routing only and could not do their own task.

In order to address these issues we can think of searching multiple trusted route between same source to destination during route formation. This allows us to use other available routes, if any route fails and also if we use some trusted route simultaneously, we may distribute the load of routing between multiple nodes. A source node will not re request for route until all trusted routes are broken or expired. In proposing a routing scheme which we named TMA-AODV (Trust based Mobility Aware AODV), we have used a number of packets successfully forwarded by a node, the number of packets delayed by a node before forwarding and number of error packets initiated by a node for trust computation. The first two parameters protect a network from any type of packet drop and packet delay attack. And the latter parameter helps us to provide a stable route. For calculating trust value, we have used weighted sum model. We have chosen AODV protocol, as it performs efficiently in both static as well as the dynamic network. For the implementation, we have used the OPNET simulator 11.0 academic edition. We have performed various analyses to understand the working of ad hoc network and AODV routing. We have implemented message drop attack and message delay attacks to study its effect on route discovery time and throughput of the network. Later on, we have investigated the proposed routing scheme (TMA-AODV) to measure route discovery time and throughput in the presence of message drop/delay attack and with and without mobility. The results of investigations show improvement in throughput and route discovery time. Route discovery time is found to be large at the beginning as the proposed scheme (TMA-AODV) has to search for multiple trusted routes from source to destination and uses them for simultaneous data transmission. Once all routes found, route discovery time improves compare to AODV. The throughput has also improved as we are detecting and avoiding packet drop and packet delay nodes while routing using TMA-AODV.

II. Brief description of the state of the art of the research topic

Mobile ad hoc networks are distributed in nature. It is a network of lightweight wireless nodes like laptop, tablet, mobile, etc. The ad hoc network is created temporary basis with no fixed or pre established infrastructure. They use wireless media (radio signals) for communication. The topology of Mobile Adhoc Network frequently changes as the nodes are mobile in nature. The packets from source node to destination node are delivered with the help of intermediate nodes if they are not in the same radio range. Each node in this network acts as a router. Routing in this network is difficult because of dynamic topology which changes with movement of nodes. Due to no controlling authority, use of radio signals as communication media and dependability of nodes to unknown intermediate nodes for packet forwarding, they are vulnerable to a number of attacks like packet dropping, packet delay, packet modification, denial of service attack etc. (Ivan Daniel Burke, R. v., 2011). The aforementioned threats are the hard security threats. The MANET also suffers from soft security threats (Kannan Govindan & P. M. ,2012). A MANET is an open system, where the nodes can enter and exit network anytime without involvement of any control or administrative authority(Adun Jøsang, 2009). The nodes have to work in coordination for proper functioning of network. In such system, it is almost impossible to define security policy (Adun Jøsang, 2009). Instead of security policy we have to think on ethical norms (Adun Jøsang, 2009). In such systems threats can be due to behaviour of the nodes, which are called soft security threats.

The existing routing protocols (AODV, DSR, DSDV, OLSR etc.) are built for mobile ad hoc network considering the mobility of nodes only. Thus, they are vulnerable to the aforementioned attacks (H Yang et. al 2004)(Adun Jøsang, 2009). We already have various mechanisms for preventing and detecting such hard security threats for wired networks (Jared Cordasco and Susanne Wetzel, 2007). However, due to limited resource of mobile node they cannot be applied to the mobile ad hoc network. Also, it will be difficult to detect/prevent soft security threats using cryptography based solutions (Adun Jøsang, 2009). We have to design some light weight technique to prevent and detect the attacker nodes and provide a stable route from source to destination. Trust based approach can be the best solution for this issue (Adun Jøsang, 2009). Many researchers proposed trust based approach for securing the Mobile ad hoc network in the last decade (A A Pirzada, C. M. 2006) (Xiaoqi Li, M. T., 2004) (A A Pirzada, A. D., 2004) (R A Shaikh, H. J., 2006) (I R Chen, J. G., 2014) (Vinesh H Patel, M. A., 2015) (Sun, M. D. 2008) (Zia, T. A. 2008) (Riaz Ahmed Shaikh, H. J.,2009) (Datta, N. M., 2012) (Mohamed M E A Mahmooud, X. L., 2013) (Gohil Bhumika, M. A., 2015). We have studied current Trust Model used for securing mobile ad hoc network and associated parameters and functions to calculate trust value. This will be helpful to distinguish the various trust model used for secure routing in MANET. This also helps to design a new approach for trust based routing in the MANET (Hosek, J., 2011).

The aforementioned hard security threats on mobile ad hoc network are categorized into two parts: Active attacks and Passive attacks. Active attacks are those which alter the content of packet and thereby disturbing the normal functioning of the network. Active attacks can be carried out by an external node or an internal compromised node which perform actions like impersonation (masquerading or spoofing), modification, fabrication and replication. Passive attacks cannot be easily detected as the attacker will not change the content of packet and the network operation is also not affected. This type of attack compromises confidentiality requirement of network communication. These active and passive attacks can be performed at any layer of the network. These attacks can be prevented using cryptographic solutions. Apart from these attacks, there may be soft security threats in MANET (Kannan Govindan & P. M. ,2012). This soft security threats are handled by trust based mechanism (Andun Jøsang, 2009) (Kannan Govindan & P. M. ,2012). In this thesis, we are concentrating on packet drop and packet delay attacks on routing in Mobile Ad hoc network. They are resource consumption attack, rushing attack, black hole attack, gray hole attack, etc. (Singh, U., 2009). The Trust based approaches do not prevent the attack. They actually detect the attacker node and avoid them in active route. The trust based scheme are also vulnerable to various trust based attacks like unfair rating attack, playbook attack, sybil attack, new comer attack etc. (Lizi Zhang, S. J., 2012).

Trust

The concept of trust comes from social science. In social science trust is defined as the subjective degree of a belief about the behaviour of a specific thing or entity (Jøsang, A. 1996). Social trust is a combination of past experience and earned reputation in society.

Trustworthiness of an entity continuously changes with time based on personal experience and situation (Jøsang, A. 1996) (Audun Jøsang 2009). (Blazed et al. 1996) addresses first the term Trust management and its role in network security. Many researchers define trust differently. For (H. Li and M Singhal 2007) trust is a belief on reliability, dependability or security. Trust is an assessment made by user to measure how well the observed behaviour of a system meets the defined standards (Jøsang, A. 1996) (Audun Jøsang 2009). In Mobile ad hoc network trust of node can be defined as how reliability, timeliness and integrity of message delivery achieved at the node's next hop (Jøsang, A. 1996). In MANET Trust modelling is the method used to establish a trust relationship among nodes of network by calculating the trust value. For calculating trust value of a node, factors influencing trust are observed and mathematical models are used (I R Chen, J. G., 2014).

Trust computation engines

Trust computation engines are used to aggregate various observations collected by a node to calculate the trust value. The most popular approaches are summation model, average model, Belief model, Fuzzy model, and Bayesian model (Audun Jøsang, 2009) (Ulieru, Z. N., 2010)

1 Summation model

It is the simplest way of calculating the trust value from collecting evidence. It simply adds the observed parameter's value to calculate direct trust. For indirect trust it collects opinion from others and add them to calculate the trust value (Audun Jøsang, 2009),

$\mathrm{Tx(Y)} = \sum_{\mathrm{i=0}}^{\mathrm{n}} \mathrm{Pi(Y)}$ Where n is the number of parameters observed and P_i is the value of the parameter.

The weighted sum model is a variation of summation model which is widely used by researcher to calculate trust value based on the importance of parameter in trust(Gohil Bhumika, M. A., 2015). In this model a weight factor with a value from 0 to 1 is associated with each parameter showing the priority or importance of that factor based on the application for which trust value is calculated. For this, actual parameter value is multiplied with its associated weight factor and they are added in final trust value. Here n is the number of parameters observed and Pi is the value of the parameter and Wi is a weight factor associated with that parameter (Gohil Bhumika, M. A., 2015).

$$\mathrm{Tx}(\mathrm{Y}) = \sum_{\mathrm{i}=0}^{\mathrm{n}} \mathrm{Wi} * \mathrm{Pi}(\mathrm{Y})$$

2 Average model

It is also a simple approach to calculate trust value of a node. In this model average of all observed parameters is calculated for computing direct trust value. Also for the indirect trust value we may do average of opinion /recommendation collected from all nodes (Audun Jøsang, 2009).

3 Bayesian model

To make any important decision an entity takes an advice from other entities who have expertise in the field or knowledge. These experts also give their advice based on accumulated knowledge, experience and other information (Audun Jøsang, R. I., 2002). The automation systems that take such decision are called expert systems. Probabilistic model can also be used to implement an expert system in which we can consider the uncertain expert knowledge to take a decision. Probabilistic model can use either classical approach in which based on repeated trials probable outcome can be find out, or Bayesian model which uses degree of persons belief that an event is occurred based on past experiences (A A Pirzadan, A.D. 2004) (Sun, M. D. 2008)(Guy Guemkam, D. K., 2013). Bayesian model is widely used to calculate trust value of a mobile node from collecting evidence and past experiences (Pirzada & McDonald, 2006)(A A Pirzadan, A.D. 2004) (Sun, M. D. 2008)(Guy Guemkam, D. K., 2013). This model is based on Bayes' rule that is used to calculate conditional probability of b given a from conditional probability of a given b.

$P\ (b|a) = (p\ (a|b) * p\ (b))\ /p\ (a)$

From Beta distribution, trust can be calculated as

$T=(p+ r_{base})/(n+p+r_{base}+s_{base})$

p is the number of positive evidences

n is the number of negative evidences

$r_{base}=s_{base} =1$

4 Belief Model

The Subjective logic trust model is introduced by A Jøsang (Audun Jøsang, T. A., 2012). The term opinion is used to represent subjective belief between two entities. An opinion can be calculated using probability which includes uncertainty. The traditional trust model does not use uncertainty. If a node doesn’t collect enough evidence about any other node, it must be uncertain about that node’s trustworthiness (Audun Jøsang, T. A., 2012). In subjective logic trust is represented using belief, disbelief and uncertainty. Opinion is a vector containing three components which defined as $w_{AB}=(b_{AB}, d_{AB}, u_{AB})$ denotes a node A’s opinion about any node B’s trustworthiness in MANET. Here first component corresponds to belief, the second component is for disbelief and third shows uncertainty. Also $b_{AB}+d_{AB}+u_{AB}=1$. To calculate values of b_{AB}, d_{AB} and u_{AB} a node will collect evidence which are positive evidence p or negative evidence n.

$b_{AB} = p/(p+n+2)$

$d_{AB} = n/(p+n+2)$ where $uBA \neq 0$

$u_{AB} = 2/(p+n+2)$

5 Fuzzy Model

In (Riaz Ahmed Shaikh, H. J., 2009) authors used this approach as trust model. This uses fuzzy logic for trust calculation. It does not include only extreme cases of node’s trust worthiness, Trusted or Untrusted but also includes the values in between these two states. For example 0.24 of trust, 0.50 of trust, trusted, untrusted.

6 Markov chain based trust model

This model is used to predict a trust value of a node from current behaviour of the node. The predicted trust value can be used only for a short period of time. Based on the current predicted state this model is used to identify the malicious behaviour of the node. Node’s state changes from one to another according to Markov chain. Author used five tuple Markov model to estimate trust value of each node (Ben-Jye Chang et al., 2008).

$\Omega= (R, V, Q, \wedge, \prod)$

R is a set of normal state $=\{r_1,r_2,r_3 \ldots r_N\}$

V is a set of malicious state $=\{v_1,v_2,v_3 \ldots v_M\}$

$Q=\{q_{ij}\}$ is a KXK matrix where K=M+N

And qij represent a transfer from i to j. i,j ϵ RUV

ʌ is a set of parameters observed and based on which state changes.

$\prod$ is $\{\prod_1, \prod_2,\ldots \prod_{M+N}\}$ set of node's initial state

$\prod_i=P0\{x(t)=r_i\}$ 1<i<N

$\prod_j=P0\{x(t)=r_j\}$ N+1<=j<=N+M and $\sum_{i=1}^{M+N}\prod i = 1$

Comparison of Existing Trust based routing approaches for Wireless Ad hoc network

1 Network Parameters used for calculating the trust value.

Each proposed technique (A A Pirzada, C. M. 2006) (Xiaoqi Li, M. T.,2004) (A A Pirzada, A. D., 2004) (R A Shaikh, H. J., 2006) (I R Chen, J. G., 2014) (Vinesh H Patel, M. A., 2015) (Sun, M. D. 2008) (Zia, T. A. 2008) (Riaz Ahmed Shaikh, H. J.,2009) (Datta, N. M., 2012) (Mohamed M E A Mahmooud, X. L., 2013) (Sonja Buchegger & Jean, 2003) (W T Luke Teacy et al, 2006) uses a number of packets forwarded by the node as one of the parameters for calculating the trust value. For this count each node will forward the packet to their immediate neighbors and get passive acknowledge them by overhearing the transmission of the next hop on route as all are in same radio range (Riaz Ahmed Shaikh, H. J.,2009). If the overheard packet matches the sent packet means the packet is successfully forwarded without modification. Some of the techniques (I R Chen, J. G., 2014) (Gohil Bhumika, M. A., 2015) (Vinesh H Patel, M. A.,2015) are using remaining battery life as one of the parameters for the trust value calculation (more battery life means more trust). This will help to choose the more stable route from source to destination. Some algorithms use the number of packets dropped by the node (I R Chen, J. G., 2014) (Gohil Bhumika, M. A., 2015) (Vinesh H Patel, M. A.,2015) (Sun, M. D., 2008) for calculating trust. If more number of packets dropped less trust value is assigned. Thus packet drop attacks (grey hole and black hole attacks) are easily detected. To detect an unnecessary delay in packet forwarding many approaches (I R Chen, J. G., 2014) (Vinesh H Patel, M. A.,2015) (Sun, M. D., 2008) (Sonja Buchegger & Jean, 2003) (W T Luke Teacy et al, 2006) use number of packets delayed by the node to calculate its trust value. More number of delayed packet forwarding reduce the trust value of node and thus detects packet delay attacks (a type of jellyfish attack). The approaches proposed in (I R Chen, J. G., 2014) (Sun, M. D., 2008) also used number of successful communication session between nodes in trust computation formula and thus quantify intimacy (social trust) relationship between them. The trust models use number of packets forwarded by node successfully, the number of packets dropped at a node, the number of packets delayed at the node and remaining battery life of node to calculate trust value of a node. All existing schemes observe or collect opinion based on one or more of these parameters to calculate trust value.

After studying all existing scheme we conclude that there has been no scientific work found which uses a number of routing error packets (RERR packets) sent by node to calculate trust. This parameter is important because if the intermediate node of any active route initiates more RERR packets means there are more link break around that node. In a MANET, one of the main reasons for link breaks is the movement of nodes. The RERR packet is created by a node of an active route when it finds a link break. The node will send the RERR packet to the source node to inform it about route failure. In response to that the source node has to research for route to the same destination. We aim to include number of RERR packet initiated by a node in the trust calculation is to detect and avoid such node during route formation and give stable route.

2 Trust computation Engines used:

Trust computation engines are meant for calculating the trust value using all observations collected by a node (Ulieru, Z. N., 2010). The most popular approaches are discussed earlier in theoretical background. The table1 shows the trust computation engine used by various existing trust based routing scheme.

3 Attacks detected:

Each existing trust based routing approaches used in wireless network (A A Pirzada, C. M. 2006) (Xiaoqi Li, M. T.,2004) (A A Pirzada, A. D., 2004) (R A Shaikh, H. J., 2006) (I R Chen, J. G., 2014) (Guy Guemkam, D. K.,2013) (Gohil Bhumika, M. A., 2015) (Vinesh H Patel, M. A., 2015) (Sun, M. D. 2008) (Zia, T. A. 2008) (Riaz Ahmed Shaikh, H. J.,2009) (Datta, N. M., 2012) (Mohamed M E A Mahmooud, X. L., 2013) (Sonja Buchegger & Jean, 2003) (W T Luke Teacy et al, 2006) successfully detects any attack which drops either data or control packets. The techniques proposed by (A A Pirzada, C. M.,2006) (I R Chen, J. G., 2014) (Guy Guemkam, D. K.,2013) (Sun, M. D. 2008) (Riaz Ahmed Shaikh, H. J.,2009) (Mohamed M E A Mahmooud, X. L., 2013) detects any modification made by attackers in packet before forwarding them. The delay in packet forwarding is detected in (I R Chen, J. G., 2014) (Vinesh H Patel, M. A.,2015) (Mohamed M E A Mahmooud, X. L., 2013) (Sonja Buchegger & Jean, 2003) (W T Luke Teacy et al, 2006) as they record total number of packets delayed by node and used it to calculate trust value. Most of the time trust based routing approaches use most trusted routes from source to destination for forwarding data packet. The trust value calculated in (Vinesh H Patel, M. A.,2015) (Gohil Bhumika, M. A., 2015) also uses remaining battery time of node and thus provide a route which has more lifetime. Also, they periodically update the trust value of the node and dynamically change the route based on new calculated trust value. Thus the same route cannot be used all the time and thus load is distributed among the nodes of the network. The trust based approach proposed in (Sun, M. D.,2008) (Guy Guemkam, D. K.,2013) uses direct trust values calculated at node using node's personal experience history and indirect recommendation provided by the other nodes. If any node tries to provide false recommendation about any other attacker node, it will be detected in this scheme. For that after receiving a recommendation from all, average of them found and if any individual recommendation is widely different than the average recommendation then it will not be considered. The following table 1 shows the description of all existing trusted based routing protocol we have studied. Table 2 shows the full form of short forms used in table 1.

Scheme	Parameters used	Routing protocol	Attacks detected/Prevented	Parameter Observed	Trust computation Engine used
A A Pirzada, C. M. 2006	NPR, NPFS	DSR	DR, MD	D	Bayesian Model
Xiaoqi Li, M. T. , 2004	NPFS	AODV	DR	I	Belief Model with Subjective Logic
A A Pirzada, A.D.,2004	NPFS	DSR	DR	D	Bayesian Model
R A Shaikh, H. J. ,2006	NPFS	AODV	DR	D & I	Average
I R Chen, J. G. ,2014	RE, NPFS, NSS, NPDR, NPD	AODV	DR, DL, MD	D	Weighted sum model
Gohil Bhumika, M. A. ,2015	MOB, RE, RT, NPDR	AODV	Load balancing, DR	D	Weighted sum model
Vinesh H Patel, M. A. ,2015	NPFS, NPDR, NPD, RE	AODV	Load balancing, DR, DL	D	Weighted sum model
Sun, M. D. ,2008	NPFS	AODV	Detects false recommendations, DR,MD	D & I	Bayesian Model
Zia, T. A. ,2008	NPFS	AODV	DR	D	Deterministic model
Riaz Ahmed Shaikh, H. J. ,2009	NPFS	AODV	DR, MD	D	Fuzzy model
Datta, N. M. , 2012	NPFS, NPR	AODV	DR	D	Average
Mohamed M E A Mahmooud, X. L. ,2013	NPFS, NPD, NPDR, NSS	DSR	DR, DL, MD	D & I	Average
Guy Guemkam, D. K. ,2013	NPFS	AODV	Detects false recommendations, DR,MD	D & I	Bayesian Model
Sonja Buchegger & Jean, 2003	Overhearing all network traffic	AODV	DR,MD	D & I	Bayesian model
W T Luke Teacy et al, 2006	NPFS, NPD	AODV	DR,MD	D & I	Bayesian model

Table 1 (Detail analysis of existing trust based routing protocols.)

NPFS	Number of packets forwarded successfully	RE	Residue Energy	D	Direct Observation
NPD	Number of packet delay	DR	Packet drop attacks	I	Indirect Recommendation
NPDR	Number of packets dropped	DL	Packet delay attack	MOB	Mobility of node
NSS	Number of successful sessions	MD	Packet modification attacks	RT	Response time
NPR	Number of packets received (to be forwarded)				

Table 2 (abbreviations used in table 1)

III. Problem Definition

Nowadays wireless ad hoc networks are getting popular for setting up network in laboratories, meeting rooms, the hostel building, etc. as they are easy to setup and no cabling or preexisting infrastructure is involved. The battery operated nodes like laptop, tablet, smart phone, etc. can be both end systems as well as a router in MANET. Routing in MANET is vulnerable to various security attacks because each node has to depend on the intermediate node for data transmission. Also, there are limited processing power, memory and battery available on the node. During data transmission an intermediate node can act as a selfish node and not forward packets for saving its own resources. Some node may unnecessarily delay packets before forwarding them to disturb the network performance. Different types of active and passive attacks may possible on mobile ad hoc network. Security mechanism used for wired network cannot be used for Mobile ad hoc network as wireless nodes are resource constrained. There must be a need for a lightweight mechanism to secure routing in MANET. Also the requirement of stable route is important to avoid unnecessary route creation process each time when the link breaks. In this thesis, we try to solve following research problem: “ How can we build a routing mechanism in a mobile ad hoc network that avoids malicious/selfish nodes in the route and give relatively stable and load balanced route considering the resource constraint nature of mobile node?” Stable route means route containing majority nodes with less mobility so that less link break. For Load balancing multiple trusted routes from source to destination are found and used simultaneously sending data packets.

IV. Objective and Scope of work

The objective of this research is

1) Analysis of routing protocols for MANET in Network Simulator to determine the choice of a routing protocol for the later research purpose.
2) Analysis of the Selected Routing protocol with UDP and TCP traffic.

3) Implementations of packet drop and packet delay attacks and study their effect on routing and network parameters.
4) Literature survey of various trust based routing schemes for comparing parameters used for trust calculation, trust computation engine used and security provided by them against various attacks.
5) From literature survey finding out research gap and come to the final problem statement.
6) Proposing a new secure and stable routing scheme with less overhead.
7) Implementing the proposed routing scheme and compare it with standard AODV routing scheme.

We define our scope as:

1) Developing selfish/malicious node in a wireless network which performs packet drop and packet delay attacks.
2) Developing a secure and stable routing protocol (TMA-AODV) for MANET. The proposed algorithm will work on the network layer.
3) We also assume that packet forwarded by a wireless node is received by all nodes who are in the range of sender node. Thus, each node monitors the network traffic of their neighbors.
4) Providing the proof of concept by improving Route discovery time of routing with TMA-AODV as a result of simultaneous usage of multiple trustworthy routes and more stable routes. Throughput is also improved with TMA-AODV in the presence of Drop and Delay attack. The improvement with TMA-AODV is to compare with AODV routing in the presence and absence of mobile nodes.

V. Original Contribution by Thesis

This thesis discusses the current trust based routing approaches and their comparative analysis for followings: Parameters used for calculating trust value, Attacks detected and Trust computation engine used for calculating the trust value. We have proposed a trust based routing protocol for mobile ad hoc network which detects both packet drop and delay activities of malicious/selfish node and establishes a stable route which has less link break. We used the weighted sum model to calculate trust value from the observed parameters because it is simple and incur less computational overhead. Also proposed routing scheme search multiple trusted paths from the same source to destination and all trustworthy paths are used simultaneously to distribute load among multiple nodes of a network. We observe the route discovery time and throughput of network in the absence and presence of malicious nodes and mobility in the network. We have also shown improvement in these observed parameters with our proposed routing protocol.

In proposed routing protocol (TMA-AODV) each node monitors traffic to and from their neighbours and stored observed values in trust table. For each neighbour node has an entry in trust table. The values observed and stored in trust table for each neighbour node is used to calculate trust value of that neighbour. This trust value specifies that how much that neighbour node is trustworthy. And this trust value will be calculated and used while the route is established from a source node to the destination node. When a source node has data to send to any destination node, it creates a RREQ packet with destination node id and send this packet to all its neighbours. If any neighbour node is destination node, it will create a RREP packet with trust value and send it to the source. Otherwise, they forward RREQ packet to their neighbours. When RREQ packet received at destination node, for each received RREQ packet a separate RREP packet is created and trust value of next hop neighbour is calculated. The trust value of RREP is initialized with the calculated trust value. Then RREP packet is sent to the next hop neighbour, who further calculates trust value of its next hop neighbour and add it to RREP trust value and send RREP to its next hop neighbour until RREP reaches at the source node. Thus, while RREP is received at each intermediate node, it will calculate the trust value of its next hop neighbour and add it into route’s trust value. So at the end source node has multiple routes towards the destination with different trust values of each route. The source node will calculate average of trust of each route and use that average as a threshold. And alternatively choose routes having greater trust value than the threshold value. Thus the load is distributed among more than one route and there will be less chance of route failure. We have modified RREP packet to accommodate trust value in it. We have also added one field in the route table entry for storing the trust value of the route.

For calculating the trust value in trust model, we have used a number of packets observed, number of packets successfully forwarded, number of packets delayed, and the number of error packets initiated. For detecting the amount of packet drop we take the difference of the number of packets observed and the number of packets successfully forwarded parameters. For detecting packet delay attack, we are interested in calculating the time taken by a node from the arrival of the packet to forwarding that packet further. If this calculated time is above the permissible delay, then our protocol detects it as a packet delay attack, i.e. A node is intentionally delaying a packet before forwarding it. Permissible delay of a packet on node is calculated by adding two delays:

processing delay and transmission delay. Processing delay is the time taken by a node to process the header of receiving a packet (CRC check etc.) and decides the output link to further forward it. The transmission delay depends on the length of packet in bits and bandwidth of the link (Abdou et al. 2015). So

$PD= D_P+D_t$

Where D_p is the time taken by node to process the packet after receiving it and D_t is the time taken by node to forward the complete packet. PD stands for Permissible Delay.

Let our ad hoc network has N number of nodes. Any random node i of a network have M numbers of neighbours. The trust table at node i has total M entries in it. One for each neighbour. Node i's trust about node j can be calculated using values stored in a trust table at node i for neighbour j.

Let $T_i(j)$ is a trust of node i about node j(j is neighbour of i).

$T_i(j) = W_1 * (Po_j-PF_j) + W_2 * Pd_j + W_3 * PER_j$

Po_j: number of packets observed for a neighbour node j,
PF_j: number of packets successfully forwarded by neighbour node j,
Pd_j: number of packets delayed at neighbour node j,
PERj: number of error packets initiated by neighbour node j,
Here W_1, W_2, and W_3 are the weight factors. $W_1+W_2+W_3=1$ and $0<= W_1, W_2, W_3<=1$. W_1 is the weight of detecting packet drop at the node which is very important as a packet drop at an intermediate node is a serious issue. W_2 is weight related to packet delay detected on the node which is less serious compare to packet drop attack. W_3 is weight related to mobility of a node. Values of weights are calculated using observed parameter values of each neighbour, using the following equation.

$X=(Po_j-PF_j) \quad Y=Pd_j \quad Z=PER_j$

$W_1=(X/(X+Y+Z)) \quad W_2=(Y/(X+Y+Z)) \quad W_3=(Z/(X+Y+Z))$

In our algorithm weight values are calculated when the trust value of any node is calculated on the node.

VI. Methodology of Research, Results / Comparisons

Methodology

1) We have studied various literatures related to trust based routing in wireless network and done a comparative analysis to find out research gap and problem statement.
2) The literature survey helped defining an objective of the research.
3) We have used OPNET 11 for implementing our proposed algorithm and performing all experiments/comparative analysis.
4) To implement our proposed routing protocols, and attacks in OPNET, we need to do following major steps. (a) Create/modify the behaviour of wireless nodes to implement attacker nodes. (b) Build/modify routing protocol and implement our proposed routing scheme.
5) In OPNET we have implemented various network scenarios and collect results and export those result values in MS Excel and use it to draw various graphs and comparisons.

Our research is **Qualitative** as we have implemented a trust based routing scheme which detects and avoids malicious/selfish activities in network and give stable route with minimum computation overhead and without incurring other communication cost.

Our research is **experimental** as we have set up MANET network scenarios with UDP and TCP of network traffic and attacker nodes (packet drop and packet delay) and prove the fairness of our proposed algorithm comparing results with standard AODV routing.

Results

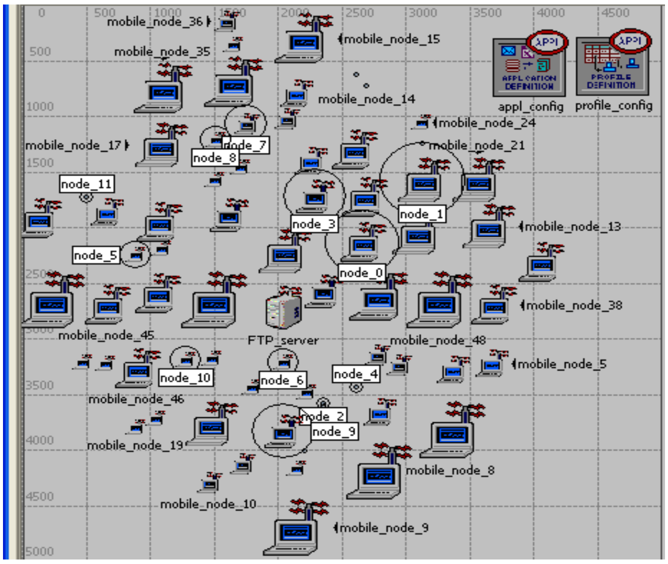
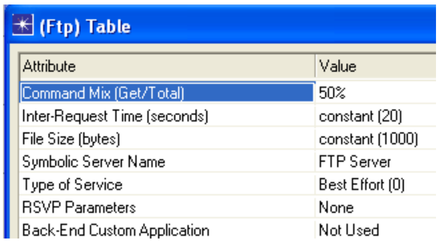


Figure 1 experiment set up (image from OPNET)

We use MANET model in OPNET to simulate AODV network. In MANET we have created two node model which performs packet drop and packet delay attack respectively. After creating the above node models, we have compared the performance of the AODV routing protocol (Route discovery time) and Wireless LAN(throughput) by creating 3 different experimental set up.

In the first experiment we have created eight scenarios as shown in figure 1(OPNET documentation). The normal scenario contains all normal nodes with AODV routing protocol. The normal scenario with all normal nodes and TMA-AODV as routing protocol. Three unreliable scenarios with 6,12 and 24 packet drop attacker nodes and AODV as routing protocol. Three unreliable scenario with 6,12, and 24 packet drop attacker nodes and TMA-AODV as routing protocol. The traffic used for simulation is TCP traffic. We have used 69 wireless nodes and one FTP server. The simulation runs for 30 minutes. All the node in the wireless LAN is fixed node. All nodes in the network are configured to run multiple FTP sessions. TCP traffic is generated by configuring the Standard FTP Applications (Application Config object) shown in figure 2 (OPNET documentation).



(Ftp) Table

Attribute	Value
Command Mix (Get/Total)	50%
Inter-Request Time (seconds)	constant (20)
File Size (bytes)	constant (1000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort (0)
RSVP Parameters	None
Back-End Custom Application	Not Used

Figure 2. Configuration of FTP traffic for more ad hoc nodes (image from OPNET)

The result obtained after the experiment is shown in table 3. For packet drop attack, we got following improvement with our proposed routing protocol. ↓ indicates decrease in value and ↑ indicate an increase in value.

	AODV		TMA-AODV		Improvement compares to AODV	
Attacker nodes	Throughput (bps)	Route Discovery time(s)	Throughput (bps)	Route Discovery time(s)	Throughput	Route Discovery time
0	350220.4	0.074528738	340092.9	0.07805756	3%(↓)	4.7%(↑)
6	308703.7	0.109340915	332235.89	0.08583977	8%(↑)	21%(↓)
12	304709.4	0.298733205	334626.29	0.17707345	9%(↑)	40%(↓)
24	264820.7	2.666962079	304009.19	0.31171683	13%(↑)	88%(↓)

Table 3 (Result obtained when Packet drop)

The second experiment setup is replica of first experiment set up. In this experiment instead of only packet drop attack, we have used half packet drop and half packer delay attacker nodes in unreliable scenarios with AODV and TMA-AODV routing. We got following results for packet drop and delay attacks. ↓ indicates decrease in value and ↑ indicate an increase in value.

	AODV		TMA-AODV		Improvement compares to AODV	
Attacker nodes	Throughput (bps)	Route Discovery time(s)	Throughput (bps)	Route Discovery time(s)	Throughput	Route Discovery time
0	350220.4	0.074528738	340092.9	0.07805756	3%(↓)	4.7%(↑)
6	327803.4227	0.113924823	340254.8	0.074694411	4%(↑)	34%(↓)
12	321633.9821	0.095035425	335520.092	0.06257037	4.2%(↑)	34.6%(↓)
24	300273.2874	0.527558508	315647.6424	0.253345187	5.3%(↑)	51%(↓)

Table 4 (Result obtained when Packet drop and delay)

The third experimental setup is the replica of second experiment set up. In this experiment out of 69 nodes we have set 20 nodes, mobile nodes with random mobility in all scenarios. We got the following results for packet drop, delay attacks and mobility. ↓ indicates decrease in value and ↑ indicate an increase in value.

	AODV		TMA-AODV		Improvement compares to AODV	
Attacker nodes	Throughput (bps)	Route Discovery time(s)	Throughput (bps)	Route Discovery time(s)	Throughput	Route Discovery time
0	321504.2126	0.094526	336514.1159	0.075984588	4.67%(↑)	19.61%(↓)
6	305048.2126	0.174754203	316856.768	0.112584966	10%(↑)	35%(↓)
12	293384.5024	0.185386923	307228.2899	0.144419099	12%(↑)	27%(↓)
24	282207.2271	0.368930013	304621.8164	0.267453009	14%(↑)	22%(↓)

Table 5 (Result obtained when Packet drop, delay and mobility)

Comparison

Comparison parameters	Sonja Buchegger & Jean 2003	A A Pirzad, A.D., 2004	Xiaoqi Li, M.T., 2004	A A Pirzada, C. M. 2006	R A Shaikh, H. J. ,2006	W T Luke Teacy et al 2006	Sun, M. D. ,2008	Zia, T. A. ,2008	Riaz Ahmed Shaikh, H. J. ,2009	Datta, N. M. , 2012	Mohamed M E A Mahmooud, X. L. 2013	Guy Guemkam, D. K. ,2013	I R Chen, J. G. ,2014	Gohil Bhumika, M. A. ,2015	Vinesh H Patel, M. A. ,2015	Our approach(TMA-AODV)
Packet drop detected?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Packet delay detected?	X	N	N	N	N	Y	N	N	N	N	Y	N	Y	N	Y	Y
Address Attack on trust value due to recommendation from others?	N	Y	N	Y	N	N	N	Y	Y	Y	N	N	Y	Y	Y	Y
Mobility of node considered?	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	Y
Load balancing among multiple route?	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y
Weighted sum model used?	N	Y	Y	Y	N	N	N	Y	N	N	N	N	Y	Y	Y	Y

Table 6 comparison of proposed routing with existing protocols

VII. Achievements with respect to objectives

- Study various existing trusts based routing scheme as part of a literature survey and compare them for parameters used for trust calculation, trust computation engine used and attacks detected.
- Define problem statement
- Study routing protocols used for MANET in OPNET and choose AODV routing for my thesis.
- Implement packet drop and packet delay attacks and study its effect on route discovery time of AODV routing and throughput of mobile ad hoc network.
- Proposed trust based routing scheme which uses a number of packets successfully forwarded, number of packets delayed and number of RERR packet initiated by the node for calculating trust. We used the weighted sum model to give priority to each parameter. The weight of parameters changes dynamically with time. Also, multiple trusted paths are searched and used simultaneously to send data.
- Implement proposed routing scheme and show improvement in route discovery time and throughput in the presence of attacker nodes and mobility.
- Compare proposed routing scheme with existing AODV routing protocol.

VIII. Conclusion

Mobile Ad hoc Networks are vulnerable to many attacks as each node of the network has to take the help of other network nodes to forward their data. Complex and computationally expensive cryptographic solution can not advisable for resource constraint MANET. For securing routing in MANET trust based scheme can be used because it is lightweight and simple.

In our proposed trust based routing scheme (TMA-AODV), we have observed total packets coming to node, total packets successfully forwarded from node, the total RRER packet initiated by a node and the total packet delayed at a node for each neighbour node and enter those parameters in trust table. On each node trust table is maintained, which stores parameters recorded for each neighbour. These values are used when the route is established in response to a RREQ by sending RREP packet. We have added a field in RREP packet, which stores the trust value of the route. When a node receives RREP packet, it calculates the trust value of next hop neighbour, using the values stored for that neighbour in trust table and this trust value will be added in the trust value of the RREP. Thus, when RREP reaches at source, the route is stored in source node's route table with the trust value associated with it.

In our proposed scheme we have used the weighted sum model for calculating trust values from observing parameters. A weight value is associated with each parameter which changes with time based on the event recorded for the node. If more packet drop recorded for a specific node more weight will be given to them while calculating trust. Same is for Delay attack and mobility.

In our proposed routing scheme all possible routes from source to destination are found. We have calculated the average of trust value associated with each route which will be threshold trust value. Source node uses all routes having trust value more than the threshold value simultaneously to send data packets. Thus the load of sending data balance among more than one route which increase network throughput and compensate with the overhead use to calculate trust value and monitoring network traffic. Since multiple trustworthy routes are found for same source and destination node in TMA-AODV, there is no need to search new route for each link breakage. We need to search for new route only when all routes break or expire. This leads to reduce route discovery time with TMA-AODV.

The result obtained from simulator also shows improvement in throughput and reduction in route discovery time with TMA-AODV in presence of drop and delay attacker nodes and in the absence and presence of mobility.

The results show that use of TMA-AODV without any attacker node and absence of mobility, reduce the throughput by 3% and increase route discovery time by 4.7% compared to AODV. This is due to overhead of modules we have added in TMA-AODV to detect and avoid attacker nodes. If we introduce 9%, 18% and 27% of total nodes attacker nodes (Drop, Drop-delay without mobility and Drop-delay with mobility) in the network, with TMA-AODV throughput is increased and route discovery time is decreased as shown in following table compare to AODV.

% attacker nodes	Drop		Drop Delay without mobility		Drop Delay with mobility	
	Throughput compared to AODV (% increment)	Route Discovery time compared to AODV (% decrement)	Throughput compared to AODV (% increment)	Route Discovery time compared to AODV (% decrement)	Throughput compared to AODV (% increment)	Route Discovery time compared to AODV (% decrement)
9	8	21	4	34	10	35
18	9	40	4.2	34.6	12	27
27	13	88	5.3	51	14	22

Table 7 improvement with TMA-AODV compare to AODV

IX. A list of all publications arising from the thesis

Sr No	Title of Paper	Conference/ Journal name
1	Trust Based Routing to avoid malicious nodes in MANET	**International Journal of Control Theory and Applications** 9 (21), 2016, pp. 105-110 **ISSN :** 0974-5572
2	Analysis of existing Trust based Routing schemes used in Wireless Network	International Journal of Information Security and Privacy (IJISP) vol 10(Issue 2) pg 24-40 April June 2016 IGI Global DOI: 10.4018/IJISP.2016040103
3	Study the effect of packet drop attack in AODV routing and MANET and detection of such node in MANET	ICT4SD 2015 Volume 1 pp 135-142 10.1007/978-981-10-0129-1_15 ISBN(print) 978-981-10-0127-7 Springer ASIC
4	Detection and avoidance of malicious node in MANET	IEEE International Conference on Computer, Communication and Control, MGI Indore, INDIA. September 10 -12, 2015 (IEEE Xplore) ISBN: 978-1-4799-8163-2 DOI: 10.1109/IC4.2015.7375729

Table 8 Publication List

X. Patents : NIL

XI. References

M. Bleze, J. Feigenbaum and J Lacy (1996), “Decentralized Trust Management” IEEE symposium on Security and Privacy pp 164-173

Jared Cordasco and Susanne Wetzel (2007),"Cryptographic vs. Trust-based Methods for MANET Routing Security" STM 2007

H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang (2004), “Security in mobile ad hoc networks: Challenges and solutions”. IEEE Wireless Communications.

Audun Jøsang (2009) Trust and Reputation Systems Tutorial at IFIP TM 2009 Purdue University

H. Li and M Singhal(2007) Trust Management in Distributed System, IEEE Computers vol 40, no 2, pp 45-53.

A A Pirzada, A. D. (2004). Trust Based Routing for ad hoc wireless networks. International Conference on Networks.

A A Pirzada, C. M. (2006). Trust establishment in pure adhoc network. wireless personal communication, 37(1-2), 139-168.

Audun Jøsang, R. I. (2002). The Beta Reputation System. 15th Bled Electronic Commerce Conference. Bled, Slovenia: 15th Bled Electronic Commerce Conference.

Audun Jøsang, T. A. (2012). Trust Transitivity and Conditional Belief Reasoning. IFIPTM 2012. Surat.

Datta, N. M. (2012). Light weight trust based routing protocol for secure ad hoc netwroks. Information Security, 6(2), 77-83.

Gohil Bhumika, M. A. (2015). Trust based service discovery in mobile ad hoc networks. Lecture notes on Software engineering, 3(4), 308.

Guy Guemkam, D. K. (2013). ARMAN: Agent based Reputation for mobile adhoc networks. Springer-Verlag Berlin Heidelberg 2013, LNAI 7879(PAAMS 2013), 122-132.

Hosek, J. (2011). Performance Analysis of MANET Routing protocols OLSR and AODV. electrorevue ISSN 1213-1539, 2(3), 22-27.

I R Chen, J. G. (2014). Trust management in mobile ad hoc network for bias minimization and application performance maximization. Ad hoc networks, 19, 59-74.

Ivan Daniel Burke, R. v. (2011). Analysing the fairness of trust based mobile adhoc network protocols(AODV and TAODV). Information Security South Africa (ISSA), 2011 . South Africa.

Jøsang, A. (1996). The right type of trust for distributed systems. ACM New security paradigm workshop, 119-131.

Lizi Zhang, S. J. (2012). Rubustness of trust models and combinations for handling unfair ratings . IFIPTM 2012. Surat.

Mohamed M E A Mahmooud, X. L. (2013). Secure and Reliable routing protocols for heterogeneous Multihop wireless networks. IEEE Transaction on parallel and distributed system, 1-11.

R A Shaikh, H. J. (2006). A trust management problem in distributed wireless sensor networks. IEEE Internatinal conference on Embedded and Real time computing.

Riaz Ahmed Shaikh, H. J. (2009). Group Based Trust Management Scheme for clustred wireless Sensor Networks. IEEE transaction on Parallel and Distributed Systems, 20(11), 1698-1712.

Singh, U. (2009). Secure routing protocol in mobile adhoc network-A survey and taxanomy. IJRIC, 7, 9-17.

Sun, M. D. (2008). probabilistic Trust management in pervasive computing. international conference on embedded and ubiquitous computing.

Ulieru, Z. N. (2010). The State of the Art in Trust and Reputation Systems: A Framework for Comparison. Journal of Theoretical and Applied Electronic Commerce Research, 5(2), 97-117.

Vinesh H Patel, M. A. (2015). Trust based Routing in Moblie Ad hoc Networks. Lecture Notes on Software Engineering, 3(4), 318.

Xiaoqi Li, M. T. (2004). A trust model based Routing protocol for Secure Ad hoc netwokrs. IEEE Aerospace Conference Proceedings.

Zia, T. A. (2008). reputation based trust management in wireless sensor network. internatinal conference on Intelligent Sensor, Sensor network and Information Procesing.

Ben-Jye Chang, S.-L. K., Liang, Y.-H., & Wang, D.-Y. (2008). Markov Chain-Based Trust Model for Analyzing Trust Value in Distributed Multicasting Mobile Ad Hoc Networks. Asia-Pacific Services Computing Conference, APSCC '08. IEEE, (pp. 151-161)

Abdou, AbdelRahman; Matrawy, Ashraf; van Oorschot, Paul (May 2015). "Accurate One-Way Delay Estimation with Reduced Client-Trustworthiness". IEEE Communications Letters. doi:10.1109/LCOMM.2015.2411591

Sonja Buchegger, J. Y. (2003). A robust reputation system for mobile ad hoc networks. EPFL-IC-LCA technical report IC/2003/50.

W. T. Luke Teacy, J. p. (2006). TRAVOS: Trust and Reputation in the Context of Inaccurate Information Sources. Autonomous Agents and Multi-Agent Systems, 12(2), 183-188.

Kannan Govindan & P. M. (2012), "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys & Tutorials (Volume: 14, Issue: 2, pages: 279 – 298).

XII Copies of papers published

Attached After this page.