ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Secured Routing For Manet Using Friend Based Adhoc Routing (FAR)

Ms.K.Deepa[1], Mrs.V.Durgadevi[2]

P.G.Scholar, Department of CSE, M.Kumarasamy College of Engineering, Karur, India[1]

Senior Assistant Professor, Department of CSE, M.Kumarasamy College of Engineering, Karur, India[2]

Abstract: One of the major problems in mobile adhoc network is to isolate the malicious node in the network. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to design a secure routing protocol over a MANET. Friend based adhoc routing using challenges to isolate the malicious node. Even though the sequential challenge was used in Friend Based Adhoc routing it is not secure. The drawback of an existing system is security cannot be provided at the MAC layer level and keys used to exchange information will be known to the attacker when he listens to the traffic. In the proposed system, before sending the data the trust value of each neighboring node is calculated by using control packet forwarding. After finding the trusted path the data will be sent to destination. Route selection is done using the trustworthiness and performance requirement of each route which is calculated based on both link capacity and traffic requirement to achieve QoS. The network performance will be greatly increased when the trust value of each node is calculated before sending the data.

Keywords: Mobile Adhoc Networks, malicious node, Friend Based Adhoc Routing, Trust Establishment, Pre distributed Keys, QoS

I. INTRODUCTION

In today's fast and rapidly growing world of technologies, more industries and businesses need the support of computer networking. Computer Networking has many classifications among these classifications wireless networks plays an important role. The main advantage brought by Mobile Adhoc Network (MANET) is mobility and scalability.

The MANET does not need any fixed network infrastructure. Infrastructureless networks have no fixed routers. It can randomly move anywhere in the network. In MANET each and every node can act as both wireless transmitter and receiver. In order to route data transmission within the network, a secure routing protocol is used to discover routes between nodes. Nodes can communicate each other directly or indirectly by use of bidirectional wireless links. The MANET has found its applications in various fields such as emergency search and rescue operations, data acquisition operations in inhospitable terrains, etc.,

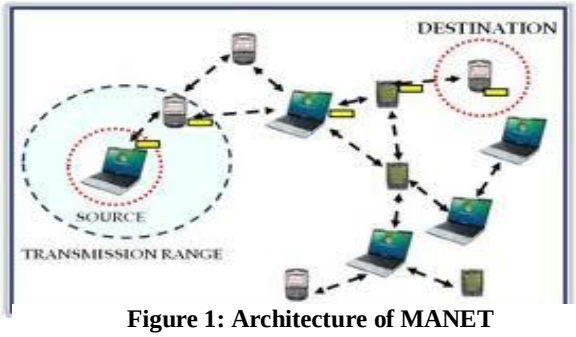


Figure 1: Architecture of MANET

Even though the mobility is provided by MANET, the communication is limited to certain areas within the communication range. This means that two nodes cannot communicate with each other when the distance between the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

two nodes is beyond the communication range is assigned to that particular node. MANET solves this problem by allowing intermediate nodes to relay data transmissions. This is implemented by dividing MANET into the following types of networks, like, single-hop and multi-hop. In a single-hop network, all parties within the same coverage area can transmit data directly with each and every node in the network, whereas, in a multi-hop network, nodes rely on other intermediate parties to transmit, if the destination node is out of their coverage area. MANET has a decentralized network infrastructure. Due to this reason a secure data transmission is required in MANET.

II. OVERVIEW

There is several research works are done on trust concept in MANETs. They are concentrated in two areas are Trust management in network and Trust including in routing protocols of MANETs. Routing Protocols in ad hoc networks there are two types of protocols are developed, they are proactive and reactive. The nodes in MANETs have limited resources therefore reactive protocols are more suitable for MANETs. The reactive routing protocol AODV is based on a hop-by-hop routing mechanism and it is a single path routing protocol. AODV is extended with multiple loop free and link disjoint method and a new protocol is developed named as AOMDV. The AOMDV proves that good improvement in the end-to-end delay and these assume that all nodes are honest and cooperative. To provide security in MANETs some cryptographic methods are introduced in AODV protocol, newly generated protocol is SAODV, but these protocols need centralized administration or trusted third party to manage network. So it is expensive and more resources are required. Recently, a new class of routing protocols in MANETs has been proposed, called trusted routing protocols, which consist of two parts: a routing strategy and a trust model. The node trust is calculated through an acknowledged mechanism from destination to source. Every acknowledged packet will increase the sender node's trusts in all the intermediate nodes along the path to the destination, whereas every retransmission decreases the trusts. It is impossible for senders to know which nodes discard packets.

There are mainly four modules in this trusted MANET: basic routing protocol, trust model, trusted routing protocol, and self-organized key management mechanism. In my work, I mainly focus on the module of trust model and trusted routing protocol. The module of trusted routing protocol contains such parts as trust recommendation, trust combination, trust judging, signature authentication routing, trusted authentication routing, and trust updating.

III. RELATED WORKS AND BACKGROUND

Generally speaking, routing algorithms can be described in two broad classes, reactive (on demand) routing and proactive (table driven) routing. Reactive protocols establish a path between the source and destination only when there are packets to be transmitted. Two commonly found reactive protocols in WSNs are Ad-hoc On-demand Distance Vector (AODV) routing and Dynamic Source Routing (DSR).Proactive protocols always have a route available, so they are more suited for dynamic networks, such as when the nodes are mobile. They are efficient if routes are used often. Reactive protocols create their routes just before data is about to be sent. This ensures the nodes have the most up to date routing information but there is a start up cost as the route is being acquired. Reactive protocols have lower overhead than the proactive protocols and work better for intermittently links.

DSDV is a proactive routing protocol based on the Bellman-Ford algorithm. It expands on Bellman-Ford by having each entry in the routing table contain a sequence number. A route is considered more favourable if it has a higher sequence number. If two routes have the same sequence number, the one with the lower cost metric is chosen. When a node decides a route is broken, it advertises that route with an infinite metric and a sequence number one greater than before. It can be shown that this routing algorithm is loop free.

DSR is a reactive protocol that is similar to AODV, the primary difference from AODV is DSR uses source routing instead of hop-by-hop routing. Each packet routed by DSR contains the complete ordered list of nodes that the packet travels through. The protocol consists of two phases, route discovery and route maintenance. Route discovery is used to obtain a path from a source to a destination. A route request packet is flooded through the network and is answered by a route reply packet. Route maintenance is used to detect if the network topology has changed.

AODV is a reactive protocol that is a combination of DSR and DSDV. Route discovery and maintenance is similar to DSR, and uses the hop-by-hop routing of DSDV. It also uses sequence numbers for loop prevention, with the goals of quick adaptation under rapidly changing link conditions, lower transmission latency that the other protocols and less bandwidth consumption.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. EXISTING FRAMEWORK

The proposed FACES protocol accomplishes establishment of friend networks in MANETs in the same way as in real life scenarios. When people meet in a new group or a community they are strangers to one another. Tasks are completed by trusting one another unconditionally initially and with time the trust level increases with the number of successful task completions. Initially breach of trust is possible. Because no one has any information about the people who is acting with malicious intentions. To avoid such a complexity, the several trust relationships are formed which leads to the formation of a community were tasks are completed efficiently[4].

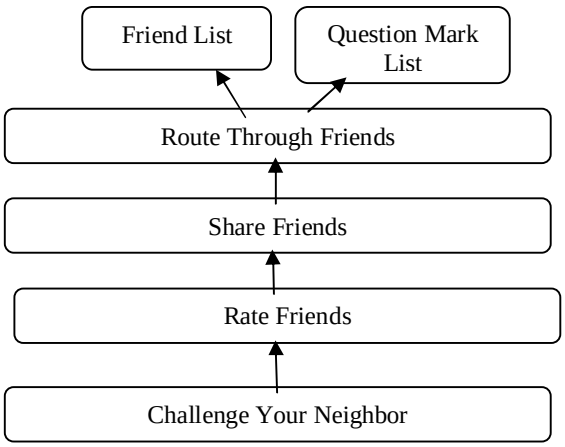


Figure 2: Stages of FACES

The FACES algorithm is divided into four stages, viz. Challenge Your Neighbor, Share Friends, Rate Friends, and Route Through Friends. The first three stages of the algorithm are periodic and the fourth one is on demand. The algorithm provides authentication of nodes by sending an initial challenge. Nodes which have completed an initial challenge will find place in the friend list. A node which does not complete an initial challenge is shifted to the question mark list. The question mark list is a list, which containing information about the malicious nodes. It signifies the misbehaving node, and it is rejected while the route selection process. The question mark list also stores the nodes which deviated from the position of friend node by performing with malicious intentions.

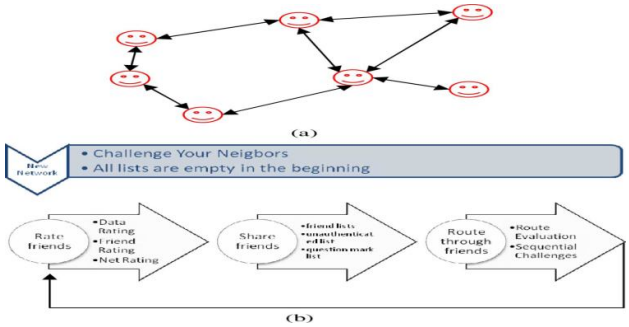


Figure 3: (a) Network of Friends in A Community (b) FACES: Link/Flow Between Different Stages

Friends are rated on the basis of the amount of data which is transferred by themselves during data transmission. While considering the rating of other friends, the rating is obtained during the friend list sharing process. The rating of friend is on a scale of between zero to ten. When a node decides to transmit data to other mobile nodes, initially it broadcasts a route request message, as required by the corresponding source routing algorithm. Each intermediate node should forwards route request message only if the sending node is not in the question mark list. On receiving the route reply messages, the source node evaluates the route by checking for friends in the route. The data is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

finally routed through the route with the greatest number of trusted friends. The quality of the route is determined by evaluating each and every node in the route and making a final decision about the quality of the route. To deal with eavesdropping the data is encrypted at the source using public key cryptography. A central authority such as a key distribution center can be very difficult to maintain in a mobile ad hoc network. So, whenever a destination node receives a route request it sends its public key along with the route reply. The source uses that public key, which it receives from the most trusted route to encrypt the data that needs to be sent. In this way the chances of man- in-middle attack are greatly reduced and eventually are eliminated as the friend circle becomes much more robust.

Even though the sequential challenge is used in Friend Based Adhoc Routing using challenge it is not secure. Because security cannot be provided at the MAC layer level and pre-distributed keys are used in FACES protocol, which means the keys used to exchange information will be known to the attacker when he listens to the traffic.

V. PROPOSED FRAMEWORK

In the proposed system, Trusted Adhoc On-demand Distance Vector Routing (Trusted AODV) is used to achieve availability of data and it provides the security at MAC layer level which greatly increases the network performance when compared to the existing protocol FACES.

Trusted AODV

Before getting into Trusted AODV, the concept of trust should be known. As an important concept in network security, trust is interpreted as a set of relations among agents participating in the network activities. These relations are founded on the proof generated by the prior interactions of entities in a protocol. As a general rule if these interactions have been true to the protocol, then trust will be accumulate between these mobile nodes. Trust has also been determined as the degree of belief about the behavior of other nodes (or agents)[3] . Establishing trust relationships among participating nodes is vital to facilitate collaborative optimization of system metrics. Trust and security are two tightly interdependent concepts that cannot be desegregated. For example, cryptography is a means to implement security but it is highly dependent on trusted key exchange mechanism. Similarly, trusted key exchange mechanism cannot take place without requisite security policies in place. It is because of this inter-reliance that both these terms are used interchangeably when defining a secure system.

TAODV [2] extends the widely used AODV (Ad hoc On demand Distance Vector) routing protocol and employs the idea of a trust model to protect routing behaviors in the network layer of MANETs. The TAODV is drawn from a network of friends. In the TAODV, trust among nodes is represented by opinion of that particular node, which is an item derived from subjective logic. The opinions of the nodes are dynamic and updated frequently as protocol specification. This protocol extends the routing table and the routing messages of ADOV with trust information which can be updated directly through monitoring in the neighborhood. When performing trusted routing discovery, unlike those cryptographic schemes that perform signature generation or verification at every routing packet, whereas in the trust model the recommended opinions together and make a routing judgment based on each element of the new opinion. In this way the computation overhead can be largely reduced, and the trustworthiness of the routing procedure can be guaranteed as well. If one node performs normal interaction with other nodes, its opinion from other mobile nodes points of view can be increased. Otherwise, if one node in the network performs some malicious activities, it will be ultimately denied by the whole ad-hoc network. A trust recommendation mechanism is also designed to exchange trust information among nodes in the network.

Network Model and Assumptions

In this work, I make some assumptions and establish the network model of TAODV. TAODV focus the security solution on routing protocol in the network layer. Mobile nodes in MANETs often communicate with one another through an error-prone, insecure wireless channel and bandwidth-limited. The following are some of the assumptions which I have made: (1) Each and every node in the network has the ability to recover all of its neighbors opinion; (2) Each node in the network can be able to broadcast some essential messages to its neighbors with high reliability; (3) Each node in the network possesses a unique ID, the physical network interface address for example, that can be distinguished from other nodes.

In the network layer, a new node model is designed as the basis of trust model. Some new fields are added into a node's routing table to store its opinion about other nodes' trustworthiness and to record the positive and negative evidences when it performs routing with others. By embedding trust model into the routing layer of MANET, the wireless scenario can save the consuming time without the trouble of maintaining the expire time, valid state, etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

which is important in the situation of high node mobility and invalidity. Also because of this reason, it is hard to design secure solutions in the transport layer, which is an end-to-end communication mechanism.

Framework of the Trusted AODV

There are mainly three modules in the whole TAODV system: basic AODV routing protocol, trust model, and trusted AODV routing protocol. Based on our trust model, the TAODV routing protocol contains such procedures as trust recommendation, trust combination, trust judging, trusted routing behaviors, cryptographic routing behaviors and trust updating. The structure and relationship among these components are shown in Figure 4. The general procedure for establishing trust relationships among nodes and for performing routing discovery is described as follows.

Let first imagine the beginning of an ad hoc network which contains a few nodes. Each node's opinion towards one another initially is (0, 0, 1) which means total uncertainty. Suppose node A wants to discover a routing path to B. Because the uncertainty element in A's opinion towards others is larger than or equal to 0.5, which means that A is not sure whether it should believe or disbelieve any other nodes, A will use the cryptographic schemes as proposed in SAODV or some other schemes to perform routing discovery operations. After some successful or failed communications, A will change its opinions about other nodes gradually using the trust updating algorithm. The uncertainty elements in its opinions about other nodes will be mostly less than 0.5 after a period of time. By means of this procedure, eventually each node in the network will form more certain opinions towards other nodes eventually after the initial time period. Once the trust relationship is established among most of the nodes in the network, these nodes can rely on our trusted routing protocol which is based our trust model to perform the routing operations.

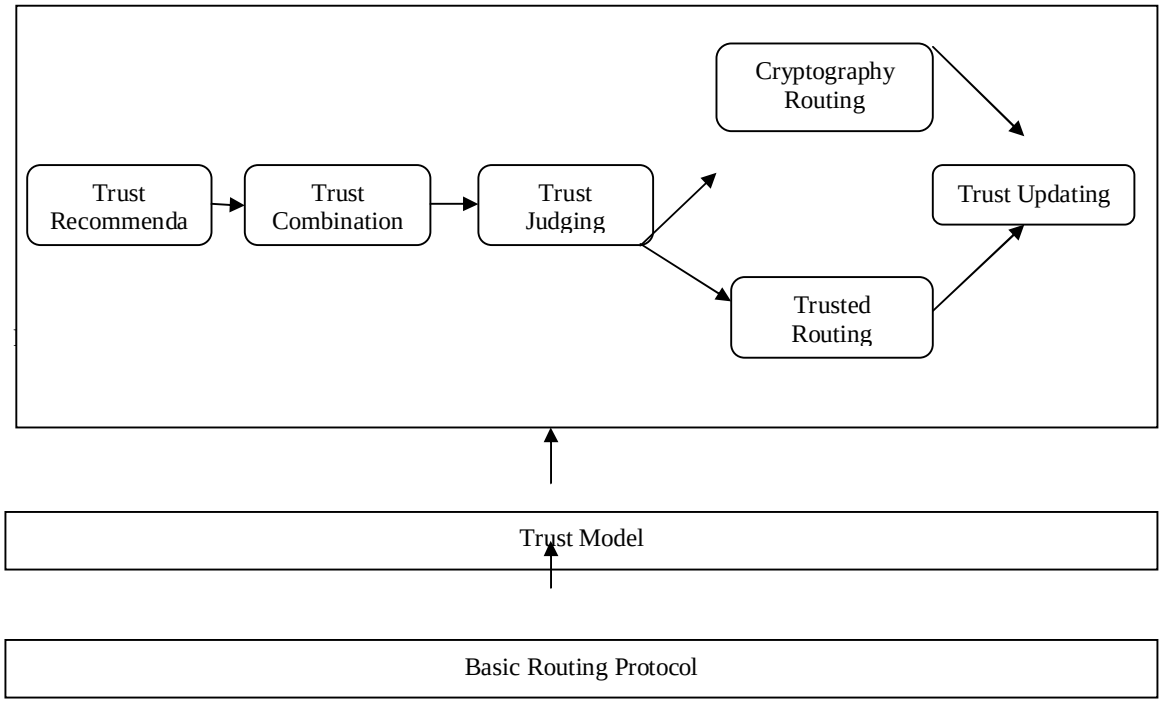


Figure 4:Framewok of Trusted AODV

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

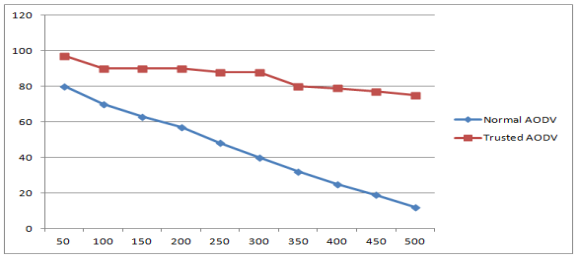
There are mainly three modules in the whole TAODV system: basic AODV routing protocol, trust model, and trusted AODV routing protocol. Based on our trust model, the TAODV routing protocol contains such procedures as trust recommendation, trust combination, trust judging, trusted routing behaviors, cryptographic routing behaviors and trust updating. The structure and relationship among these components are shown in Figure 4. The general procedure for establishing trust relationships among nodes and for performing routing discovery is described as follows.
Let first imagine the beginning of an ad hoc network which contains a few nodes. Each node's opinion towards one another initially is (0, 0, 1) which means total uncertainty. Suppose node A wants to discover a routing path to B. Because the uncertainty element in A's opinion towards others is larger than or equal to 0.5, which means that A is not sure whether it should believe or disbelieve any other nodes, A will use the cryptographic schemes as proposed in SAODV or some other schemes to perform routing discovery operations. After some successful or failed communications, A will change its opinions about other nodes gradually using the trust updating algorithm. The uncertainty elements in its opinions about other nodes will be mostly less than 0.5 after a period of time. By means of this procedure, eventually each node in the network will form more certain opinions towards other nodes eventually after the initial time period. Once the trust relationship is established among most of the nodes in the network, these nodes can rely on our trusted routing protocol which is based our trust model to perform the routing operations.

Node A now will utilize the trust recommendation protocol to exchange trust information about a node, B, from its neighbors, then use the trust combination algorithm to combine all the recommendation opinions together and calculate a new option towards B. The subsequent routing discovery and maintenance operations will follow the specifications of our trusted routing protocol. In this framework, the establishment of trust relationships among nodes and the discovery of routing paths are all performed in a self-organized way, which is achieved by the cooperation of different nodes to exchange information and to obtain agreements without any third-party's interventions.
Features of TAODV (Trusted AODV)
The following features are provided by Trusted AODV

(1) The mobile 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)The system performance is improved by avoiding requesting and verifying certificates at every routing step.
(4) It is more secure and having better performance than AODV. It can prevent modification, fabrication attack.

VI. SIMULATION ANALYSIS

To increase the network performance in MANET a new routing protocol is designed. The data's are selected and transferred from the source to the destination via the intermediate mobile nodes. In order to compare the performance of Trusted AODV (TAODV) and normal AODV, both protocols are run under identical mobility and traffic scenarios.



Packet Delivery Ratio vs. Number of Nodes
Figure 5: Packet Delivery Ratio Graph where node varies 1 to 500

The packet delivery ratio of the normal AODV and TAODV is compared for different set of nodes. As per the graph the packet delivery ratio of the Trusted AODV is increased when compared with the normal AODV.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VII. CONCLUSION

Trust in the network is nothing but the faith of one node on other node. Trust based path is secured to use and increase the confidentiality of data being transferred. In this paper, trust based Adhoc On-Demand Routing protocol is proposed. An extra field that is routing table is introduced. This field indicating trust value is updated on every successful data transmission. The data transmission is based on the route selection value which is calculated. This route selection value is used to select most trusted path rather than selecting shortest or longest path. This improves the trust factor of one mobile node on the other nodes in the network significantly. This is useful in forthcoming communication in the network. I have conclude that the trust based routing protocol proposed in this paper enhance the security level at MAC layer and also improves the network performance. This paper suggests some modification in the working of AODV routing protocol in the direction of enhancing security level.

REFERENCES

[1] Pankaj Sharma, Yogendra Kumar Jain, "Trust Based Secure Aodv In MANET" Journal of Global Research in Computer Science Volume 3, No. 6, June 2012
[2] R. S. Mangrulkar, Pallavi V Chavan S. N. Dagadkar "Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MANET", International Journal of Computer Applications (0975 – 8887) Volume 7– No.10, October 2010
[3] K. Seshadri Ramana Dr. A.A. Chari Dr. N.Kasiviswanth "Review and Analysis of Trust Based Routing in MANET", IJCSR International Journal of Computer Science and Research, Vol. 1 Issue 1, 2010.
[4] Sanjay K. Dhurandher, Mohammad S. Obaidat, Fellow, IEEE, Karan Verma, Pushkar Gupta, and Pravina Dhurandher, "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems", IEEE systems journal, vol. 5, no. 2, June 2011
[5] Ahmed Mohamed Abdalla, Ahmad H. Almazeed, Imane Aly Saroit, Amira Kotb "Detection and Isolation of Packet Dropping Attacker in MANETs", International Journal of Advanced Computer Science and Applications, Vol. 4, No.4, 2013
[6] Balakrishna.R, U.Rajeswar Rao, N.Geethanjali, "Detection of Routing Misbehavior in MANETs", IEEE communications surveys & tutorials, vol. 11, no. 4, fourth quarter 2010
[7] Caroline Sheedy, "Privacy Enhanced Protocols using Pairing Based Cryptography", Thesis, January, 2010
[8] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE communications surveys & tutorials, vol. 10, no. 4, fourth quarter 2010
[9] Mangrulkar Pallavi.R.S, V. Chavan, S. N. Dagadkar, "Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MANET", International Journal of Computer Applications (0975 – 8887) Volume 7– No.10, October 2010
[10] Radhika Saini, Manju Khari "Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network", International Journal of Computer Applications (0975 – 8887) Volume 20– No.4, April 2011
[11] Seshadri Ramana.K, Dr. A.A. Chari, Dr. N.Kasiviswanth, "Review and Analysis of Trust Based Routing in MANETs", International Journal of Computer Science and Research, Vol. 1 Issue 1, 2010
[12] Soufiene Djahel, Farid Nait-abdesselam, and Zonghua Zhang, "Mitigating Packet Dropping Problem in MANETs", in IEEE communications surveys & tutorials, vol. 13, no. 4, fourth quarter 2011