IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 3, March 2015.
www.ijiset.com
ISSN 2348 – 7968

Trusted Routing with an Efficient Certificate Revocation for Mobile Ad Hoc Network

R. Yasodharan[2], R. Sivabalakrishnan[1] and P. Devendran[3]

[1]Assistant Professor, Department of Mechatronics Engineering,
SNS College of Technology, Coimbatore, India
[2]Assistant Professor, Department of Mechatronics Engineering,
SNS College of Technology, Coimbatore, India
[3]Assistant Professor, Department of Mechatronics Engineering,
SNS College of Technology, Coimbatore, India

Abstract

Connecting through mobile increased steeply in last few years. Hence the necessary for secured communication is also given higher priority. This dissertation work aims in improving the security and the quality of service for mobile ad hoc network by providing Trusted Routing. Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. Mobile Ad-hoc networks (MANETs) have various characteristics like mobility, infrastructure less, spontaneously created and can be established in any environment without pre-existing infrastructure with ease of deployment. Due to these characteristics of MANETs they can be used for various applications. However to use MANETS in commercial purpose they must be secured from malicious attackers. Providing security to MANETs is difficult due to vulnerability of wireless links, the limited physical protection of nodes and the dynamically changing topology.

The scope of this paper is to provide a trusted infrastructure in the clustered network which makes secure and reliable packet forwarding, especially for providing quality of service (QoS). To improve the security of MANET the idea is to develop trust establishment between the cluster of nodes or among neighboring cluster nodes. In this trusted infrastructure, the malicious node or intruder is detected directly by the cluster head and it is recovered back. The detected nodes can further participate in the communication process and route discovery process. The measurements of quality of service were taken as end-to-end latency, energy, packet delivery ratio and the communication overheads. The simulation is carried out using network simulator version-2 by using Ad hoc On Demand Distance Vector (AODV) protocol.

Keywords: *Mobile Ad-hoc, network, Trusted routing, MANETS,*

1. INTRODUCTION

Wireless technologies have grown to be popular that exhibits ubiquitous features, fulfilling the demand of network communication anywhere, at anytime. Since portable devices like laptop computers, personal digital assistance (PDAs) and mobile phones require fixed infrastructure such as access point or base stations, therefore they need an access to a static network to support their mobile device services. To provide a solution to this problem Mobile Ad hoc Networks (MANETs) have evolved. An ad hoc network is a multi-hop wireless communication network supporting mobile users without any existing infrastructure. To become commercially successful, the technology must allow networks to support many users. A complication is that addressing and routing in ad hoc networks does not scale up as easily as in the Internet. By introducing hierarchical addresses to ad hoc networks, it can effectively address this complication. Trust in MANET can be derived by observing the behavior of other nodes. Different methodologies are used to observe behavior to take the evidence and to calculate the trust for particular node.

D. Umohoza et al [16] has projected a trust based scheme in which trust can be computed based on quality of service (QoS) parameters. Probabilities of transit time variation, deleted, multiplied and inserted packets, processing delays are used to estimate and update trust. Functions which facilitate this are provided and evaluated. Pedro B. Velloso et al [12] has proposed the trust based scheme based on based on previous individual experiences and on the recommendations of others. The Recommendation Exchange Protocol (REP) which allows nodes to exchange recommendations about their neighbours is presented.

Jian Wang et al [5] have projected different trust computation techniques instead of packet dropping ratio. In this technique the similarity degree between nodes is used as a trust metrics like velocity, moving directions, and affiliated organization and it gives good performance in mobile conditions but the limitations is that it is complicated to select the similarity attributes for computations of trust as far as the security is concern. Bo Wang et al [8] has proposed a trust based routing scheme in which the packet delivery ratio as a trust metrics the link quality is considered to provide QoS guarantee. So the proposed method ensures the forwarding of packets through the trusted and least link delay routes only by monitoring the behavior of neighboring nodes and meeting the QoS constraint accordingly. But the limitation is that it is vulnerable to false recommendation attack and also trust metrics does not provide the better QoS guaranty.

Elhdhili et al [3] propose a clustering algorithm to elect trusted, stable and high-energy cluster head (CH) called clustering algorithm for security in ad hoc networks

ISSN 2348 – 7968

which creates one-hop members to minimize the overhead and consider the trust level of nodes, mobility, remaining energy and distance. Peng et al [13] proposes Voting-based clustering algorithm which is another trust-based clustering scheme which evaluates stability of node through computing the neighbor change ratio and the residual power of nodes. In this scheme, each node votes other nodes only if the node is the most trustful one among its neighbor nodes. Votes are propagated only to one hop neighbors and they are not forwarded by other nodes.

Kadri et al [8] proposes a secured weighted-based clustering scheme which is another method which elects cluster heads according to their weight computed by combining a set of parameters such as stability, battery, degree and etc. Zae-kuwn et al [18] recommended a QoS aware routing and power control algorithm consuming low transmission power for multimedia service over ad hoc network. Then proposes an effective routing and power control algorithm for multimedia services that satisfies end-to-end delay constraint with low transmission power consumption.

Jeffery et al [5] describe an approach for satisfying application specific QoS expectations operations on ad hoc networks where available bandwidth fluctuates. The proposed distributes QoS Resource allocation model incorporates a distributed optimization heuristic that results in near optimal adaptation without the need to know, estimate, or predict available bandwidth at any moment in time.

This protocol is mainly to alleviate the scalability issue with respect to communication overhead in implementing source routing. Instead of disseminating the state of each link network wide, each node broadcasts its node status (including its current position, velocity, moving direction, and available resources on each of its outgoing links) across the network periodically or upon a significant change. With such information, at any instant each node can locally depict an instant view of the entire network. To accommodate a QoS request, the source locally computes a QoS satisfied route (if available) and route data packets along the calculated path. Moreover, the source can predict route break and predicatively compute a new route before the old route breaks by using the global state it stores. This routing protocol is suitable for providing soft QoS in small or medium sized networks wherein mobile hosts are equipped with Global Positioning System (GPS) receivers and their moving behavior is predictable.

2. FUNDAMENTAL

2.1 MANET

MANETs are autonomous systems consisting of mobile hosts that are connected by multi-hop wireless links. MANETs are decentralized networks that develop through self-organization. MANETs are formed by a group of nodes that can transmit, receive and relay data among themselves. In mobile ad hoc network there is no fixed infrastructure therefore the mobile hosts communicate over multi-hop wireless links. These are often called infrastructure-less networking since the mobile nodes in the network dynamically establish routing paths between themselves. The overview of MANET communication is shown in the Figure1.

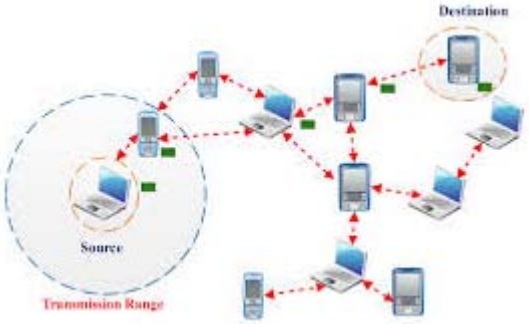

Figure 1. Mobile Ad hoc Network

Topology control deals with the problem of maintaining a connected topology among the nodes in ad hoc networks. This covers power control and hierarchical topology organization. In power control network connectivity is ensured by altering the power of each node in order to balance one-hop neighbour connectivity whereas hierarchical topology control is an approach referred to as clustering.

2.2 Clustering in MANET

Clustering provides a method to build and maintain hierarchical addresses in ad hoc networks. Clustering refers to a technique in which MANET is divided into different virtual group; generally nodes which are geographically adjacent are allocated into the same cluster driven by set of protocols based on behaviors and characteristics of the node. This enables the network to become manageable. Various clustering techniques allow fast connection and also better routing and topology management of MANET.

2.3 Trust Concepts

Trust is an important aspect of mobile ad hoc networks. It enables entities to cope with uncertainty and uncontrollability caused by the free will of others. Trust computations and management are highly challenging issues in MANETs due to computational complexity constraints, and the independent movement of component nodes. This prevents the direct application of techniques

ISSN 2348 – 7968

suited for other networks. In MANETs, an untrustworthy node can wreak considerable damage and adversely affect the quality and reliability of data. Therefore, analyzing the trust level of a node has a positive influence on the confidence with which an entity conducts transactions with that node.

3. SYSTEM ANALYSIS AND DESIGN

The cluster based certificate revocation with vindication capability (CCVRC) scheme is used with the help of voting based mechanism and the threshold based mechanism. In the CCVRC scheme any node can be accused by any member in the cluster by sending accusation packet. The cluster head receives the accusation packet and keeps the accused nodes in the warned list and accusing node in the black list. The certificates of those nodes are revoked and the nodes that are in the list cannot participate in communication process and packet forwarding. In voting mechanism, if the cluster head receives the accusation packet against a node, it will revoke its certificate. In this voting mechanism the cluster head takes only the first accusation, this accusation may or may not be correct. The threshold mechanism is used to release the falsely accused node; if the threshold value is high the falsely accused node may take time to release. If the threshold is less, the chance of releasing the malicious node is more.

The major limitation in CCVRC schemes are in the voting based mechanism all the nodes in the cluster must vote honestly. All the nodes or cluster members in the cluster must actively participate in the voting process to accuse a node. The threshold mechanism is not reliable, because here the malicious node which is accused may be released falsely. The nodes that in the warned and black list must not participate in communication process. The accused node may act as misbehavior node due to less energy, or loss of communication to the next nodes.

4. PROPOSED METHODOLOGY

The main objective for designing the system is to apply cluster based certificate revocation scheme which is to detect the malicious node and the intruders. In addition it permits the detected cluster member (node) and the malicious node for further participating in the network communication. All the legitimate nodes are pre loaded with the certificate, which means an encrypted data is provided to all the legitimate nodes which will be provided by the cluster head during cluster formation. The encryption of the data is done by using bit swapping mechanism.

The simple trust model is introduced in the clustering technique which acts as an intermediate to forward the packet from a source node to the destination node. Trust relies on the fact that the trusted entities do not act maliciously. This trust model provides a platform that the nodes that have never met before can communicate with each other based on a mutual trust relationships developed over a period of time and enhances the quality of service metrics.

The methodology applied to achieve the security and the trusted routing as follows

Step 1: Mobile nodes are deployed in the specified geographical area.
Step 2: Apply the Weighted Clustering Algorithm to form the cluster.
Step 3: Apply Bit Swapping Mechanism to pre load the certificate.
Step 4: Apply the trust model to evaluate the trust degree between nodes.
Step 5: Apply AODV protocol for the route discovery and route maintenance.
Step 6: Introducing malicious node to evaluate the security of the entire network.
Step 7: Evaluate and compare the performance of the quality of service metrics from statistical values obtained from simulation results.
Step 8: Analyses the results.

5. SYSTEM ARCHITECTURE

5.1 Cluster Formation

The weighted clustering mechanism selects cluster heads by considering important aspects related to the efficient functioning of the system components. Therefore, in order to optimize battery usage, load balancing and medium access control functionality a node is chosen to be a cluster head according to the number of nodes it can handle, mobility, transmission power and battery power. To avoid communications overhead, this algorithm is not periodic and the cluster head election procedure is only invoked based on node mobility and when the current dominant set is incapable to cover all the nodes. To ensure that cluster heads will not be over-loaded a predefined threshold is established in order to specify the number of nodes each cluster head can ideally support. WCA selects the cluster heads according to the weight value of each node. The weight associated to a node v is defined as

$$W_v = w_1\_v + w_2 D_v + w_3 M_v + w_4 P_v$$

The node with the minimum weight is selected as a cluster head. The weighting factors are chosen so that $w_1 + w_2 + w_3 + w_4 = 1$. M_v is the measure of mobility. It is taken by computing the running average speed of every node during a specified time T. _v is the degree difference. _v is obtained by first calculating the number of neighbours of each node. The result of this calculation is defined as the degree of a node v, dv. To ensure load balancing the degree difference _v is calculated as |dv − _| for every

node v. The parameter D_v is defined as the sum of distances from a given node to all its neighbours. This factor is related to energy consumption since more power is needed for larger distance communications. The parameter P_v is the cumulative time of a node being a cluster head. P_v is a measure of how much battery power has been consumed. A cluster head consumes more battery than an ordinary node because it has extra responsibilities. The cluster head election algorithm finishes once all the nodes become either a cluster head or a member of a cluster head. The distance between members of a cluster head, must be less or equal to the transmission range between them.

If a node proclaims itself as Cluster Head (CH), it propagates a Cluster Head Hello Packet (CHP) to notify neighboring nodes periodically. The nodes that are in the Cluster Heads transmission range can accept the packet to participate in this cluster as cluster members. On the other hand, when a node is deemed to be Cluster member (CM), it has to wait for Cluster Head Packet (CHP). Upon receiving CHP, the CM replies with a CM Hello Packet (CMP) to set up connection with Cluster Head (CH). Afterward, the CM will join in the cluster; meanwhile, CH and CM keep in touch with each other by sending CHP and CMP in the time period T_u.

5.2 Detection of Malicious Node and the Intruders

To detect the malicious node and the intruder, the certificate of that node plays a vital role. The certificate of the node is preloaded by the cluster head using bit swapping mechanism which uses exclusive OR operations. The restrictions in the simulation environment are as follows: The cluster Member must not communicate to any other cluster member. If the cluster member communicates to some other cluster member who does not belong to the same cluster it is said to be the intruder. The cluster head verifies the group id of the intruder and detect it any sending the recovery packet. Until the detection of the intruder the remaining cluster must not communicate to it. When the malicious node enters into the cluster and communicates with the cluster member, the communicated cluster member is treated as intruder since it does not have permission to communicate. Here the cluster head verifies the certificate of the malicious node and detect it. Once the detection process is over the cluster member can communicate to the detected node and involve in packet forwarding.

5.3 Simple Trust Model for forwarding the Packets

Each node derives a trust degree value for each neighbors that how frequent it responses to the requested node. This value is the measure of the level of trust in its neighbor. For the purpose of scalability, the trust degree value is calculated using the local information. Let $T_{ij}(t)$ denote the degree of trust node of node i its neighbor j at time t. The trust degree value is limited to a continuous range from 0 to 1. The trust degree 0 denotes complete distrust whereas the value 1 represents absolute trust. The weighted average takes two parts:

$$T_{i,j}(t)=W_1T_i^d{}_j(t)+W_2T_i^r{}_j(t)$$

$T_i^d{}_j(t)$ represents the direct trust degree of node i in node j based on node i's direct observation of node j's packets forwarding behavior at time t. $T_i^r{}_j(t)$ denotes the indirect trust degree that neighbors of node i have in node j by recommendation at time t. These neighbors of node i are also neighbors of node j. The weight factors W_1 and W_2 (W_{1+} W_2=1, $0\leq W_1\leq$ 1and $0\leq W_2\leq 1$) are assigned to $T_i^d{}_j(t)$ and $T_i^r{}_j(t)$, respectively. This simple trust model helps in forwarding the packets with the mutual relationship. The trusted node never acts maliciously and it delivers the packet to the destination securely.

5.4 Ad-Hoc on Demand Distance Vector Protocol (AODV)

AODV is described in [20]. It's reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network. There are three types of control messages in AODV which are discussed below.

5.4.1 Route Request Message (RREQ)

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

5.4.2 Route Reply Message (RREP)

A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

5.4.3 Route Error Message (RERR)

Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

5.5 Route Discovery Mechanism in AODV

When a node "A" wants to initiate transmission with another node "G" as shown in the Fig. 3.1 , it will generate a route request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forwarded to the neighbors, and those node forward the control message to their neighbors' nodes.

ISSN 2348 – 7968

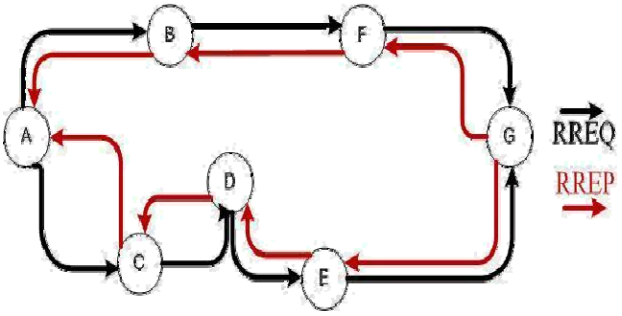

Figure 3.1 AODV Route Discovery

This process of finding destination node goes on until it finds a node that has a fresh enough route to the destination or destination node is located itself. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is established between "A" and "G", node "A" and "G" can communicate with each other Figure 3.1 depicts the exchange of control messages between source node and destination node.

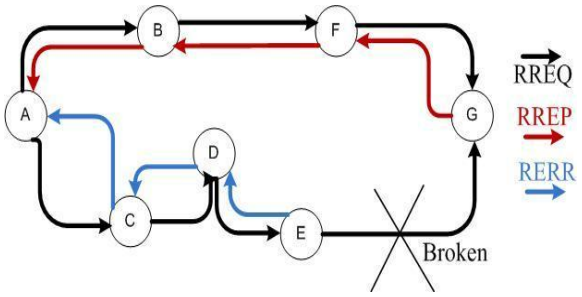

Figure 3.2 Route Error Message in AODV

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating the destination node i.e. from the node "A" to the neighbors nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error, where "A" is source node and "G" is the destination node. The scheme is shown in the Figure 3.2

6. RESULTS AND DISCUSSION

Resource utilization and security in MANETs is of prime importance in several scenarios of deployment such as battlefield, event coverage, etc. One of the primary goals is to provide trusted routing and the detection of malicious node is to prevent the compromised nodes in the network from disrupting the route discovery and maintenance mechanisms. This idea is used in the clustered network to achieve the performance of the network. The trusted route is discovered within the two hop communication range, so the cluster member from one group can straightforwardly communicate to the sink with the help of trusted node which acts also a gateway node. This trusted route increases the performance of the quality of service and makes the communication faster. The simulation results of An Efficient Certificate Revocation with Trusted Routing for Mobile Ad hoc Network is to detect the malicious node and the quality of service is compared with existing CCVRC: Cluster based Certificate Revocation with Vindication scheme.

6.1 Detection of malicious node and intruders

The detection of malicious node and the intruder is detected with the help of certificate which is provided by the cluster head. During the cluster formation, the cluster head is elected by using the least weight. The cluster head identifies its neighbor nodes by sending "HELLO" message for a certain time interval. Once the communication is established among the cluster member and cluster head, the certificates of each node is pre-loaded by the cluster head. The cluster head monitors the cluster member, when it finds the misbehaving cluster member being detected by revoking the certificate.

Figure 4.1 Identification of the intruder

The nodes are placed in the simulation environment and the clusters are grouped according the weight of the cluster members. In the Figure 4.1 the cluster member 11 is communicating with another cluster member 17. This cluster member violates the rule and moreover, this happens before the cluster head election. Both the cluster member will be communicating until it is detected by the cluster head.

ISSN 2348 – 7968

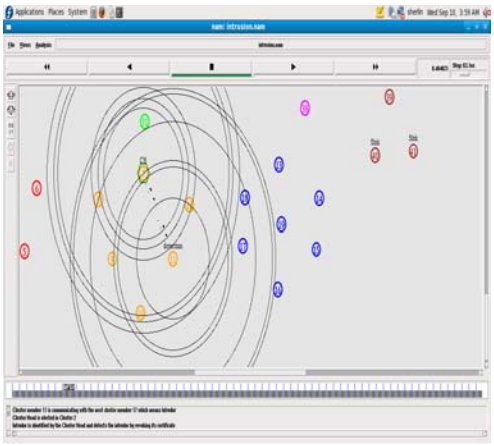

Figure 4.2 Detection of the intruder

After a certain period of time the cluster head 7 starts communicating with that intruder 11 and detects the intruder by revoking its certificate. When the detection process is over, the detected cluster member 11 stops its misbehaving communication activities in the network.

Figure 4.3 Identification of Malicious Node

In the Figure 4.3 malicious node 0 is a mobile node which does not belong to the cluster group. Now it starts it communication to cluster member 22 and that cluster member 22 also starts to communicate with that malicious node 0 so it is treated as intruder. Malicious node initiates it communication to another cluster member 21. In the mean time cluster head 20 monitors those cluster members and detects it by revoking its certificate. By revoking the certificates of the malicious node and the intruders cannot involve in misbehaving activities.

6.2 Trusted Routing for forwarding the packets

The trusted node is identified during the communication period and each node derives a trust degree value for each neighbors node that are within the transmission range. The trust degree value is consider from 0 to 1 which means that if node is having a trust degree 1 it is treated as trusted node. The trusted node may acts also a gateway node, this helps in sending packets from one cluster to another cluster in a reliable manner.

Figure 4.4 Forwarding packets through trusted node

In Figure 4.4 cluster head 20 sends its packet through the trusted node 24 in its own cluster (acting as a gateway) and makes it to transfer packet to the next cluster head 26. The reason why it stops to the next cluster head is: because that cluster head 20 have enough transmission range so, it cannot directly sends all packets to the sink, if it tries to forward more that its transmission range it will be dropped. The cluster head 26 waits until it receives all the corresponding packets from the cluster head 20.

Figure 4.5 Forwarding packets to the next cluster head

In Figure 4.5 the Cluster head 26 sends the entire received packet to the next cluster head 35. Now the cluster head finds its route through the trusted node 28.

ISSN 2348 – 7968

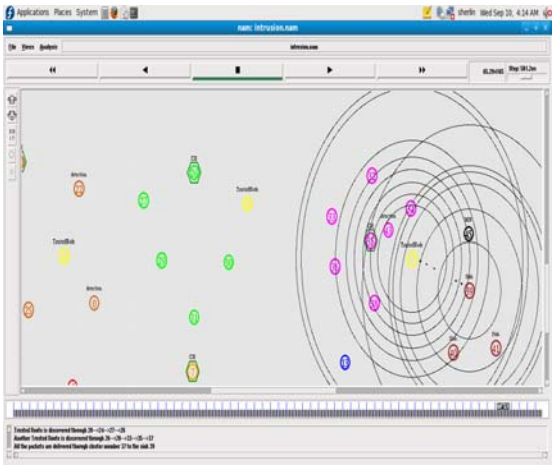

Figure 4.6 Packets reached to the sink through the entire trusted node

In Figure 4.6 all packets are safely reached to the sink without any interruption of the malicious node. By sending the packets through the trusted node enhances quality of service and reduces the communication overheads. The simulation results are compared with the existing work to evaluate the performance of the proposed work. In Network simulator, the performance evaluation is as follows: when the simulation is over a trace file is generated. From the trace file the required parameters are analyzed using awk script and perl command.

6.3 Packet Delivery Ratio

Packet Delivery Ratio is calculated by analyzing the trace file which is generated after the simulation is over. The packet delivery ratio is considered as numbers of packets received at the destination by number of packets send from the source into 100. The greater value of packet delivery ratio means the better performance of the system. The Figure 4.7 shows the comparison result of the existing work and the proposed work

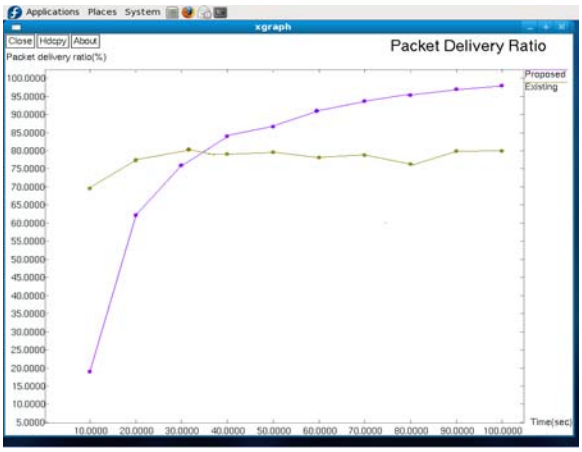

Figure 4.7 Packet Delivery Ratio

6.4 End to End Latency

The average time taken by data packets to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. The lower value of end to end delay means the better performance of the system. The Figure 4.8 shows the comparison result of the existing work and the proposed work.

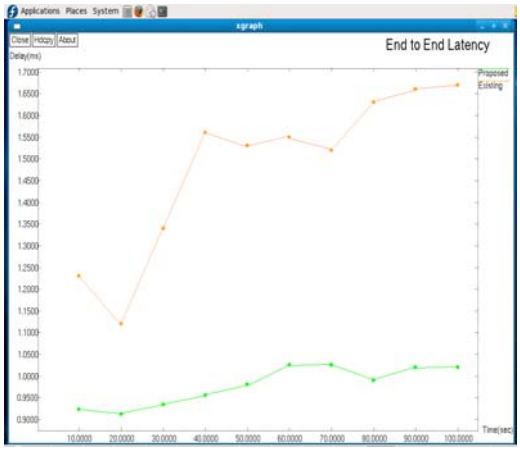

Figure 4.8 End to End Latency

6.5 Energy Consumption

The average energy consumed on idle state, sleeps state, transmit time and received time by the total energy consumed. In mobile ad hoc network the nodes moving and keeps communicating with the neighbors makes much of energy. In the below Figure 4.9 shows the energy consumption in the sleep state and idle state is comparison result of the existing work and the proposed work. Energy is consumed much comparing to the existing system. Energy consumption is measured in joules.

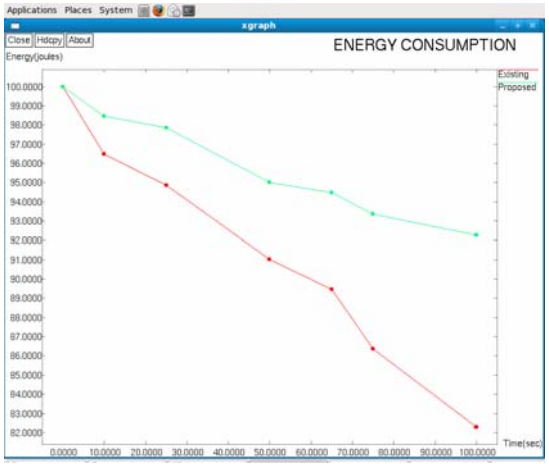

Figure 4.9 Energy Consumption

ISSN 2348 – 7968

6.6 Overall Performance of CCVRC Scheme and Certificate Revocation with Trusted Routing for Mobile Ad hoc network

Performance Metrics	Cluster based Certificate Revocation with Vindication Capability	An Efficient Certificate Revocation with Trusted Routing for Mobile Ad hoc Network
Malicious Node Attack Rate	High	Reduced
Packet Delivery Ratio	low	Increased
End to End Latency	High	Reduced
Energy Consumption	High	Reduced
Control Overheads	High	Reduced

Table 4.6 Comparison of results

Malicious node attack rate, Packet Delivery Ratio, Control Overheads, Energy Consumption, End to End Latency are taken for comparison. Packet delivery ratio is measured in terms of percentage, End to end latency is measured in terms of seconds, Energy is measured in terms of joules, and overheads are measured in terms of Overheads. Table 4.6 shows the comparison of performance metrics between existing and proposed work.

When comparing the results of the existing system and the proposed system, the parameters which are taken for analyze shows the better performance.

5.1 CONCLUSION

Various issues in MANET are due to dynamic infrastructure and no centralized administration makes such network more vulnerable to many attacks. In this research, how the malicious node and the intruders in the clustered network are identified is discussed. The malicious node may enter into the cluster group and may damage the network by raising some attacks. Before raising those attacks and degrades the performance of the network, the malicious nodes and the intruders within cluster are identified directly by the cluster head and revoke its certificate. In addition to this the trusted route is discovered and the packets are forwarded through the trusted node using simple trust model. The simple trust model derives a trust degree value for each of its neighbor nodes. The node which has more trust value is selected as a trusted node. An Efficient Certificate Revocation with Trusted Routing improves the overall performance of the quality of service using Ad hoc On Demand Distance Vector Protocol.

5.2 FUTURE WORK

In the proposed work the security of the clustered network is enhanced and the quality of service metrics such as packet delivery ratio, energy consumption, control overheads, end to end latency and malicious node attack rate are increased. Further improvements can be done as follows:

- Key management Infrastructure can be introduced to provide different types of certificates to different cluster members.
- The future research work focus on the Quality of Service Routing algorithms and protocols.
- Trust Agent can be introduced to derive a trust degree for each cluster members and broadcast the trust value for the requested member.

BIBLIOGRAPHY

[1] Bo Wang, Chuanhe Huang, Layuan Li, et al., “Trust-based minimum cost opportunistic routing for Ad hoc networks”, Journal of Systems and Software - 2011.
[2] T. Camp, J. Boleng, and V. Davies. “A Survey of Mobility Models for Ad Hoc Network Research" - 2002.
[3] M. E. Elhdhili, L. B. Azzouz and F. Kamoun, “CASAN: Clustering algorithm for security in ad hoc networks”, Computer Communications - 2008.
[4] K. Fall and K. Varadhan, “The NS Manual”, The VINT Project, UC Berkeley - 2002.
[5] Jeffery P.Hansen Scott, Plakosh Daniel, Wrage Lutz, Adaptive quality of service in ad hoc wireless networks,IEEE Wireless Communications and networking Conference -2012.
[6] Jian Wang, Yanheng Liu, Yu Jiao, “Building a trusted route in a mobile ad hoc network considering communication reliability and path length”, Journal of Network and Computer Applications - 2011.
[7] Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen, “A survey on trust management for mobile ad hoc networks”, IEEE Communications Surveys and Tutorials, 2011.
[8] B. Kadari, A. Mhamed and M. Feham, “Secured Clustering Algorithm for Mobile Ad Hoc Networks”,

ISSN 2348 – 7968

IJCSNS International Journal of Computer Science and Network Security - 2007.
[9] Kannan Govindan, Prasant Mohapatra," Trust computations and trust dynamics in mobile ad hoc networks: a survey", IEEE Communications Surveys and Tutorials, 2012.
[10] N. Marchang, R. Datta,"Light-weight trust-based routing protocol for mobile ad hoc networks", IET Information Security - 2012.
[11] Omkumar. S., Rajalakshmi. S." Analysis of Quality of Service using Distributed Coordination Function in Aodv", European Journal of Scientific Research – 2011.
[12] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, et al., "Trust management in mobile ad hoc networks using a scalable maturity-based model", IEEE Transactions on Network and Service Management-2010.
[13] S. Peng, W. Jia and G. Wang, "Voting-Based Clustering Algorithm with Subjective Trust and Stability in Mobile Ad-Hoc Networks", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing - 2008.
[14] C. Park, Y. Lee, H. Yoon, S. Jin and D. Chio, "Cluster based Trust Evaluation in AdHoc Networks", pp. 503-507.
[15] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate revocation to cope with false accusations in mobile ad hoc networks", - 2011.
[16] D. Umuhoza, J.I. Agbinya, C.W. Omlin ,"Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms", AusWireless 2007.
[17] L. Xu, X. Wang and J. Shen, "Strategy and Simulation of Trust Cluster Based Key Management Protocol for Ad hoc Networks", Proceedings of 4th International Conference on Computer Science & Education - 2009.
[18] Zae-kwun Lee, Gyeongcheol Lee, Hwangjun Song, QoS-aware routing and power control algorithm for multimedia service over multihop mobile ad hoc network, Wireless Communications and Mobile Computing - 2012.
[19] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in IEEE INFOCOM, 2005.

Yasodharan. R received his B.E. degree in Electronics and Communication Engineering and M.E. degree in Mechatronics Engineering. He is currently pursuing his `Ph.D. in the area of Renewable resources. Having 5 years of experience in PCB industry, he is expert in PCB designing and PCB Manufacturing. He is currently serving as an Assistant Professor in SNS College of Technology, Coimbatore from 2012. His research interests include Solar Tracking system, Robotics, Process control and PCB designing. He is a Life Member of the International Association of Engineers (IAENG), International Society for Research and Development (ISRD), International Association of Computer Science and Information Technology (IACSIT). His works published in 4 International Journals and several conference proceedings

Sivabalakrishnan.R was born in Erode, India, in 1986. He received the B.E. degree in Electrical and Electronics Engineering from the VCET, India, in 2009, and the M.E. degrees in Mechatronics Engineering from Kongu engineering College, India, in 2012. He joined the Department of Mechatronics Engineering, SNS College of Technology, as a Assistant Professor, and in 2013 became a member of three professional bodies. He has presented two papers in national and international conference in the year 2012. He has published two papers in international journals.

Devendran P, Assistant Professor, SNS College of Technology. He have two years research experience in the field of welding by the use of different types of algorithms. He published the research paper in two international and 6 national conferences. Completed Master of Engineering in Mechanical discipline and Bachelor of Engineering in Mechatronics.