Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.132 – 142

RESEARCH ARTICLE

Improving Security to avoid Malicious Node for Reducing Routing Overhead in Mobile Ad Hoc Networks (MANET)

ANANDRAJ D.S

PG Student, Dept of CSE, Sri Krishna College of Technology, Coimbatore, India

P.Madhavan

Assistant Professor, Dept of CSE, Sri Krishna College of Technology, Coimbatore, India

ABSTRACT

Ad-hoc Network is new paradigm of wireless communication for mobile host. In MANETs some of the nodes do not take part in forwarding packets to other nodes to conserve their resources such as energy, bandwidth and power. The nodes which act selfishly to conserve their resources are called selfish nodes. The selfish nodes are engaged to reduce data availability and produce high communication cost in terms of query processing. Many selfish node detection methods are found to detect the nodes which do not participate in packet forwarding but they fail to detect the selfish nodes which does not allocate replica for the purpose of other nodes. Paper provides methods to detect selfish nodes in terms of allocating replica to other nodes. The methods are categorized according to detect the selfish nodes and reduce the impact of that nodes in mobile ad hoc network.

Keywords: Certification Authentication, Mobile ad hoc networks, Malicious, neighbor coverage, network connectivity, routing overhead

1. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. No base stations are supported in such an environment. Due to considerations such as radio power limitation, channel utilization, and power-saving concerns, a mobile host may not be able to communicate directly with other hosts in a single-hop fashion. In this case, a multi hop scenario occurs, where the packets sent by the source host are relayed by several intermediate hosts before reaching the destination host. However, due to node mobility in MANETs, frequent link breakages may lead to frequent path failures and route discoveries. It increases the

overhead of routing protocols which reduces the packet delivery ratio and also increases the end-to-end delay. Thus, reducing the routing overhead in route discovery is an essential problem. The conventional on demand routing protocols use flooding to discover a route. They broadcast a Route Request (RREQ) packet to the networks, and the broad casting induces excessive redundant retransmissions of RREQ packet.

MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. There is no central administration to take care of detection and prevention of anomalies in Mobile ad hoc networks. Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources.

2. RELATED WORK

2.1 THE EXISTING SYSTEM

A rebroadcast delay is calculated to determine the rebroadcast order, and can obtain the more accurate additional coverage ratio by sensing neighbor coverage knowledge. An approach combines the advantages of the neighbor coverage knowledge and the probabilistic mechanism, which can significantly decrease the number of retransmissions so as to reduce the routing overhead, and can also improve the routing performance.

Xin Ming Zhang, En Bo Wang, Jing Jing Xia, and Dan Keun Sung et al [1] Broad casting is an effective mechanism for route discovery, but the routing overhead associated with the broadcasting can be large, especially in high dynamic networks. The protocol analytically and experimentally, and showed that the rebroadcast is very costly and consumes too much network resource. Optimizing the broadcasting in route discovery is an effective solution to improve the routing performance. Network density is high or the traffic load is heavy, the improvement of the gossip-based approach is limited, proposed a probabilistic broadcasting scheme based on coverage area and neighbor confirmation. Coverage area to set the rebroadcast probability, and uses the neighbor confirmation to guarantee reachability. Scalable Broadcast Algorithm (SBA) is rebroadcast of a packet according to the fact whether this rebroadcast would reach additional nodes. Dynamic Probabilistic Route Discovery (DPR) is based on Neighbor coverage and each node determines the forwarding probability according to the number of its neighbors and the set of neighbors which are covered by the previous broadcast.

Limitations

Neighbor coverage knowledge includes additional coverage ratio and connectivity factor.

Dynamically calculate the rebroadcast delay, which is used to determine the forwarding order and more effectively exploit the neighbor coverage knowledge.

Jae-soo Kim , Qi Zhang and Dharma P. Agrawal et al [2] A dynamic probabilistic broadcasting approach with coverage area and neighbor confirmation , the coverage area concept to adjust the rebroadcast probability of a node. One of the earliest broadcast mechanisms is flooding, where every node in the network retransmits a message to its neighbors upon receiving it for the first time. Although flooding is extremely simple and easy to implement, it can be very costly and can lead to serious problem, named as broadcast storm problem, which is characterized by redundant packet retransmissions, network bandwidth contention and collision. Neighbor knowledge scheme maintains neighbor node information to decide whether it or the neighboring nodes have to rebroadcast or not. To use neighbor knowledge method, each node has to explicitly exchange neighborhood information among mobile hosts using periodic Hello packets. Four different gossip versions are presented for ad hoc routing (GOSSIP1 (p, k), GOSSIP2 (p1, k, p2, n), GOSSIP3 (pψkψm)is just like GOSSIP1 (pψk), GOSSIP4 (pψkψk') is just like GOSSIP1 (pψk)). In general, Neighbor knowledge methods perform better than Area based methods, while Area based methods perform better than Probability based methods.

Limitations

An important problem is how to minimize the number of rebroadcast packets while good retransmission latency and packets reachability are maintained.

Even though the large number of rebroadcasts guarantees high reachability, it causes high network bandwidth wastage and so many packets collisions.

On the other hand, the small number of rebroadcasts results in low reachability, because it cause rebroadcast chain broken so that some hosts may not receive the broadcast packets.

Abdulai, J. and Ould-Khaoua, M. and Mackenzie, L.M. and Mohammed, A et al [5] Routing overhead associated with the dissemination of routing control packets such as RREQ packets can be quite huge, especially when the network density is high and the network topology frequently changes. Issue of reducing the routing overhead associated with the route discovery and maintenance processes in on-demand routing protocols has attracted increasing attention. Location Aided Routing (LAR) algorithm as an approach to mitigate the route discovery overhead by utilizing location aided information for mobile nodes, location information can be obtained using the global positioning system (GPS) receivers. The localization of prior routing histories to localize the RREQ flood to a limited region of the network, Routing On-demand Acyclic Multi-path (ROAM) protocol mitigates the number of retransmissions of RREQ floods by using directed acyclic sub-graphs based upon the distance between the source and destination nodes. The construction and maintenance of virtual

backbone that guarantees total coverage of the entire network is either based on Connected Dominating Set (CDS) or Cluster based algorithms. A predefined probability value to decide whether or not to forward an RREQ packet. Some optimizations such as two-threshold scheme (i.e. use higher probability value for nodes with fewer neighbors) are introduced to prevent broadcast packets from quickly dying out and/or prevent nodes from transmitting excessive packets.

Limitations

A dynamic probabilistic route discovery using AODV as the base routing protocol, which traditionally uses the blind flooding.

In order to reduce the routing overhead without degrading the network throughput, especially in dense networks, the forwarding probability of nodes located in sparse areas is set high while it is set low at nodes located in dense areas.

Zygmunt J. Haas, Senior Member Joseph Y. Halpern, and Li (Erran) Li et al [6] Gossiping to ad hoc unicast routing, it's usage of gossiping is very different from the work, try to ensure that messages are eventually delivered, even if there is no connected path between the source and the destination at any given point in time. Exists a path using communication links at some point in time, messages can be delivered through a random pair-wise exchanges among mobile hosts. Using gossiping mechanism to improve multicast reliability in ad hoc networks, they do not use gossiping to reduce the number of messages sent. Flooding is a basic element in many of the ad hoc routing protocols, as mentioned and comparing gossiping to flooding.

Limitations

Gossiping can save in terms of overall traffic depends on the gossip probability used, node mobility, and the type of messages sent.

Protocol is simple and easy to incorporate into existing routing protocols, by adding gossiping to AODV, significant performance improvements in all the performance metrics, even in networks as small as all nodes.

Craig Gentry et al [8] Novomodo and related proposals are improvements over CRLs and OCSP, infrastructural requirements of these approaches can vary dramatically, depending on how users use their keys. First, since third party queries can come from anywhere and concern any client, every certificate server in the system must be able to ascertain the certificate status of every client in the system. One way to achieve implicit certification in the encryption context is identity based encryption (IBE). An IBE scheme uses a trusted third party called a Private Key Generator (PKG).The main algorithms in IBE are as follows Private key generation: For a given string ID, PKG uses (s, Paramus, ID) to compute the corresponding private key dID. Encryption: Sender uses (params, ID, M) to compute C, cipher text for M .However, there are two negative consequences: 1) private key escrow is inherent in this system – i.e., a PKG can easily decrypt its clients' messages; and 2) the PKG must send client private keys over secure channels, making private key distribution difficult. Decryption: Client uses (Paramus, dID , C) to recover M .

Limitations

The certificate-based encryption (CBE), which combines public-key encryption (PKE) and IBE while preserving most of the advantages of each.

This certificate has all of the functionality of a conventional PKI certificate (even of a signature key),but it can also be used as a decryption key.

A.M. Hegland, E. Winjum, C. Rong, and P. Spilling et al [9] Single Administrative Domain (SAD) involved operations refer to operations where all involved parties belong to the same regime or share a common, predefined point of trust. Multiple Administrative Domains (MAD) involved operations represent operations involving ad hoc partners, that have had no prior contact and belong to different organizational/security domains. Key management operations should finish in a timely manner despite a varying number of nodes and node densities, fraction of the available bandwidth occupied by network management traffic should be kept as low as possible. Any increase in management traffic reduces available bandwidth for payload data accordingly. Wired network solution is a public key infrastructure (PKI) where a centralized certificate authority (CA) issues certificates binding the public keys to specific users/nodes. Self-Healing Session Key Distribution (S-HEAL) is a symmetric group key-distribution scheme with revocation, designed for networks with unreliable links. Logical Key Hierarchy (LKH) Group keys can be updated brute force; a group manager distributes the new group key, encrypted with a separate (individual) key for each node. Probabilistic Key Pre-distribution (PRE) assumes WSN nodes outfitted with a preinstalled key ring, that is, a set of keys drawn randomly from a large pool of keys, When bootstrapping the network, the nodes broadcast the identifiers of the keys in their key ring.

Limitations

Classify key-management schemes for MANETS (mobile ad hoc networks) as either contributory or distributive.

Distributive schemes based on symmetric techniques are either intended for traditional MANETs or for wireless sensor networks (WSNs).

Observation is that none of the proposed key-management schemes for MANETs are truly effective for all MANET scenarios.

Genevie`ve Arboit, Claude Cre´peau, Carlton R. Davis, Muthucumaru Maheswaran et al [11] Ad-Hoc network security schemes which utilized certificates that rely on hierarchical trust model, do not explicitly address the issue of certificate revocation, Other proposals such as make the assumption that periodic access to on-line CAs is available; therefore CRLs can be obtained from the CAs. In Buchegger and Le Boudec proposed the CONFIDANT protocol that is aimed at detecting and isolating misbehaving nodes, methodology for actually computing the trust level or rating of the nodes within a MANET. A number of reputation systems have been published in research literature, systems can be divided into two main types: centralized and distributed reputation systems. Centralized reputation systems require central authorities for collecting the rating of participants and derive reputation scores. Centralized reputation systems are not suitable for MANETs since MANETs do not have

centralized entities. The majority of proposed decentralized reputation systems are transactional based; that is, they require inputs, such as size of upload or down files, quality, price and upload/ download experiences relating to interactions of providers of services and users of the services. Our scheme stipulates that before entering a network, the MANET nodes must have a valid certificate from a recognized CA, as well as the public keys of the CAs which issued certificates for potential network peers.

Limitations

Presented a decentralized certificate revocation scheme which utilizes certificates that are based on the hierarchical trust model.

Delegates all key management tasks except the issuing of certificates—to the nodes in a MANET and it does not require any access to on-line certificate authorities (CAs)

Certificate revocation scheme is based on weighted accusations; whereby a quantitative value is assigned to an accusation to determine its weight.

Vignesh.M, Sujay.E.K, Tharanya.M, Saranya.R, D.Jayachandran et al the paper, propose a neighbor coverage-based probabilistic rebroadcast protocol with implementation of good node detection algorithm for reducing routing overhead and energy consumption in MANETs. Many routing protocols, such as Ad hoc On-demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR), have been proposed for MANETs. Energy efficiency is one of the main problems in a mobile ad hoc network, especially designing a routing protocol. The proposed work aims at discovering an efficient energy aware routing scheme in MANETs. All information related with good neighbors is stored in routing table which improves performance of routing protocol in terms of good communication and stable route. Analytical results of proposed solution shows that it improves data throughput, improve overall performance of the network and improve network life with in fixed and dynamic transmission range.

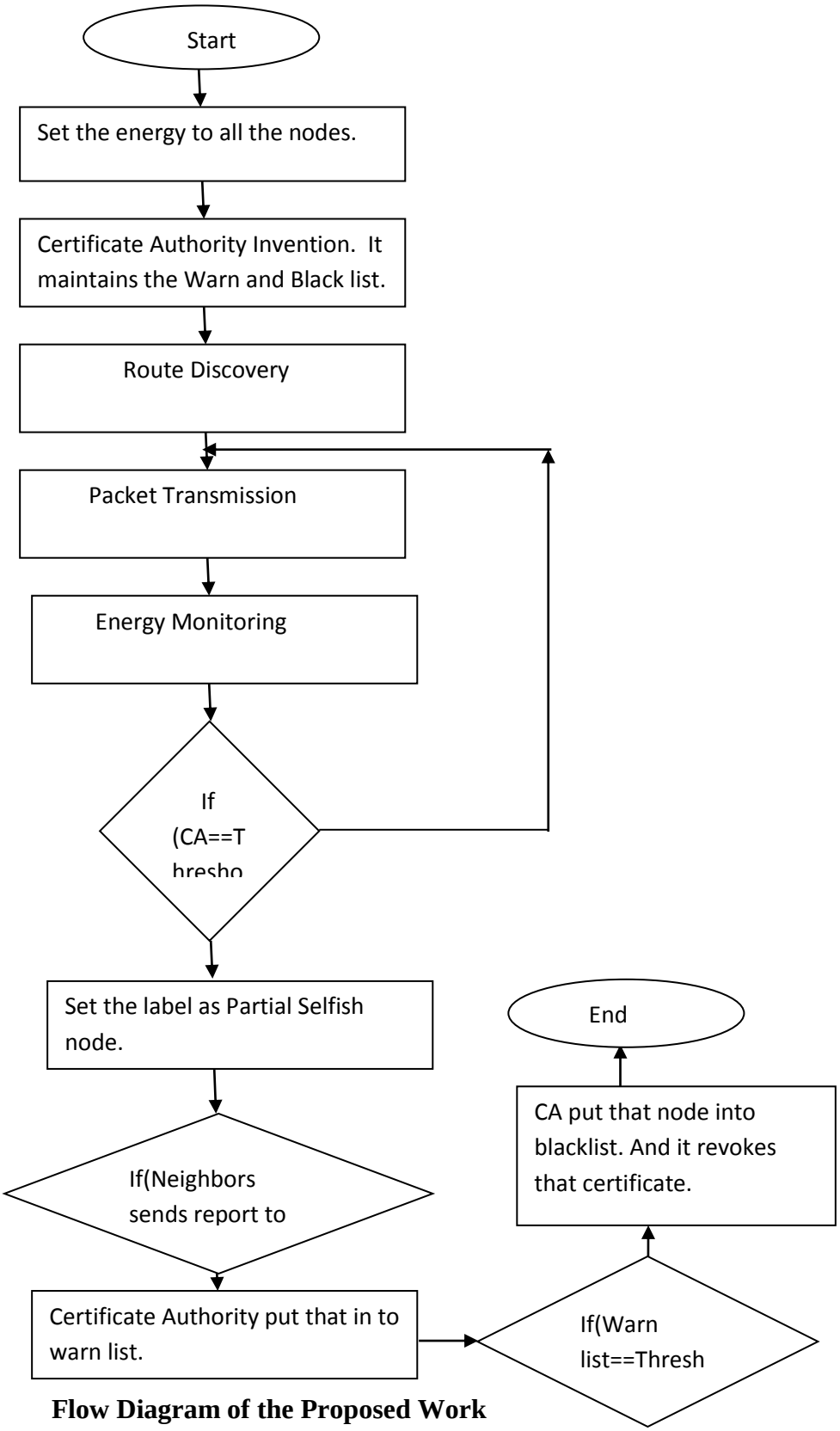
PROPOSED SYSTEM

GNDA (Good Node Detecting Algorithm) is used to detect the selfish nodes and the Malicious nodes. It improves overall performance of the network with in fixed and dynamic transmission range.

ADVANTAGES

1. Selfish node detection
2. Malicious node detection

Flow Diagram



Flow Diagram of the Proposed Work

IMPLIMENTATION

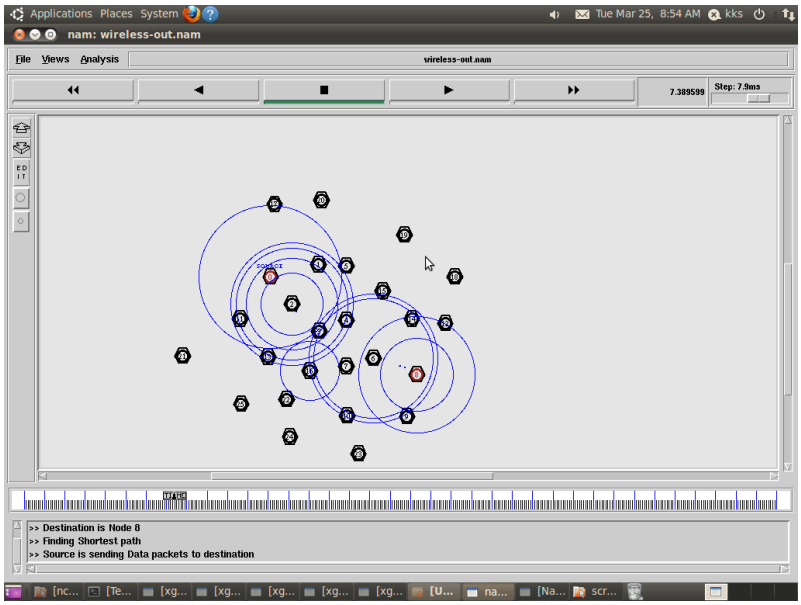


Fig 1 Discovering Nodes for Routing.

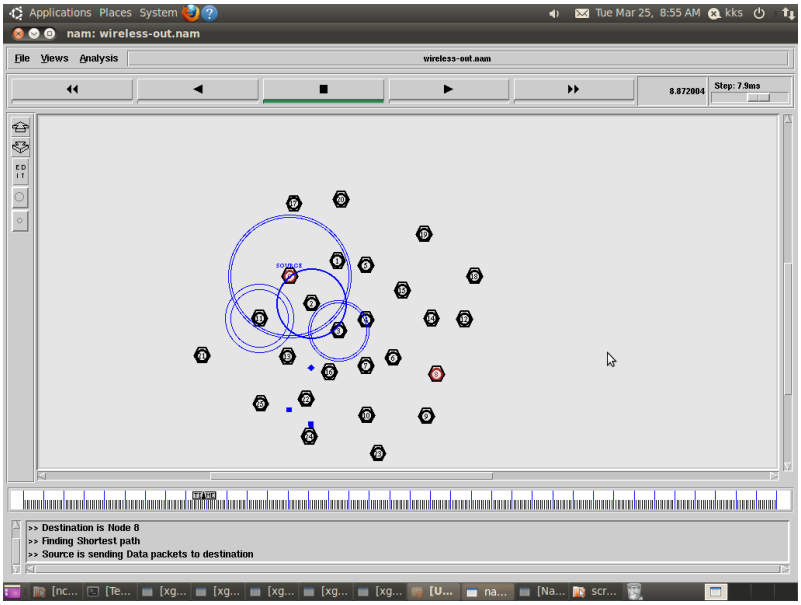


Fig 2 Packet loss by Decreasing Energy in node.

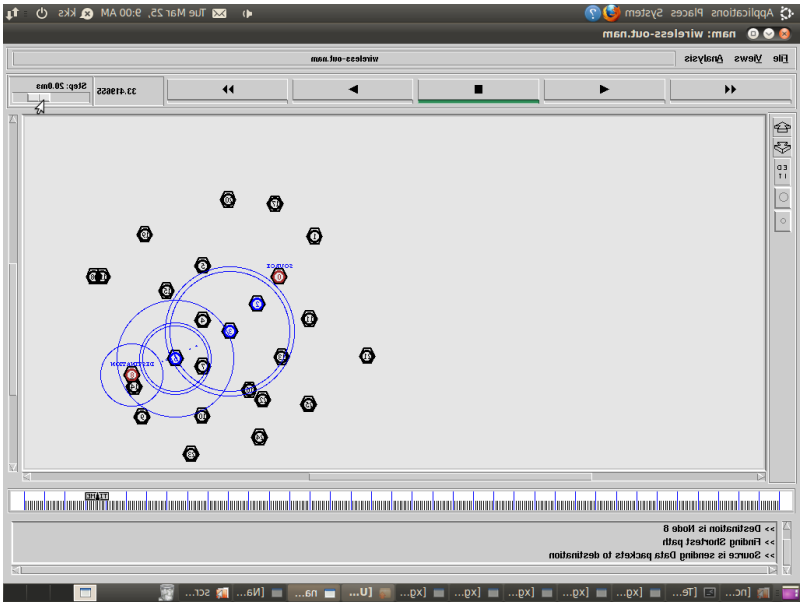


Fig 3 Data routing without Selfish nodes

PERFORMANCE AND EVALUATION

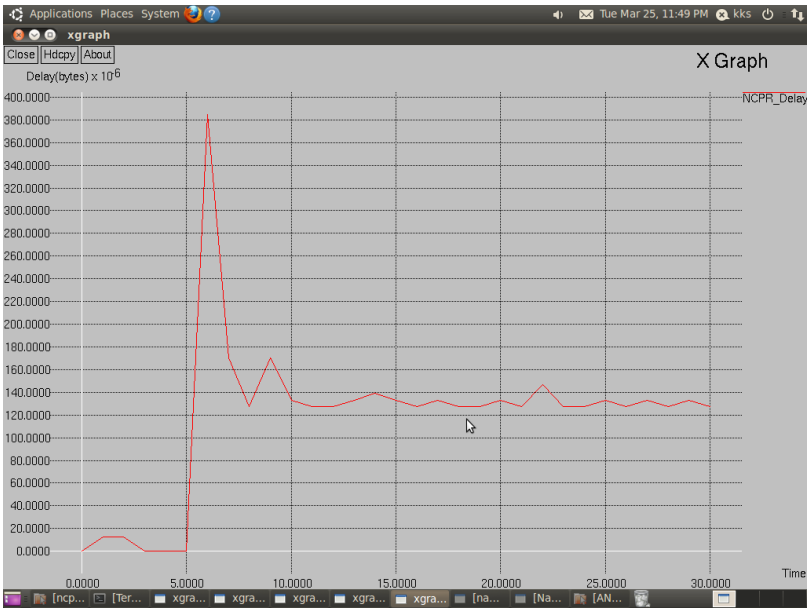


Fig 4 Delay for Neighbor Coverage Probabilistic Routing.

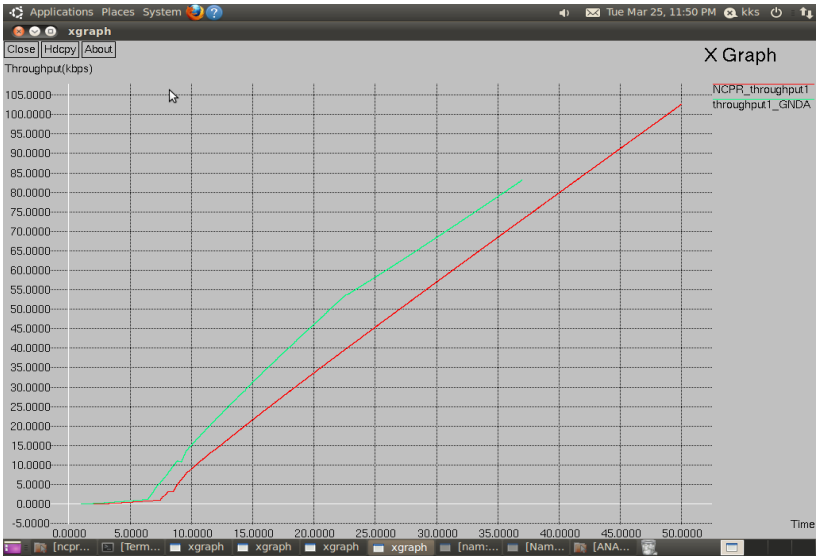


Fig 5 Comparison Throughput for NCPR and Selfish Node.

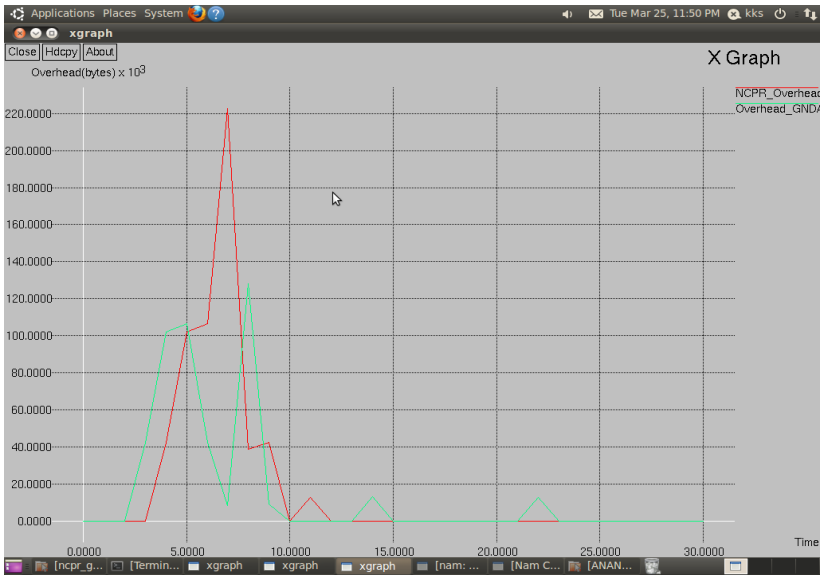


Fig 6 Comparison of Routing Overhead for NCPR and Selfish Node.

CONCLUSION

A probabilistic rebroadcast protocol based on neighbor coverage to reduce the routing overhead in MANETs. This neighbor coverage knowledge includes additional coverage ratio and connectivity factor. To dynamically calculate the rebroadcast delay, which is used to determine the forwarding order and more effectively exploit the neighbor coverage knowledge. GNDA algorithm has been created. It selects the nodes which should have the maximum energy. With the help of this algorithm, selfishness problem has been avoided. And in this, Certificate authority has been introduced. It is used to detect the malicious nodes

that are also known as misbehaving nodes. Simulation results show that the proposed system generates less delay and less rebroadcast traffic than the flooding and some other optimized scheme in literatures. Because of less redundant rebroadcast, the system mitigates the network collision and contention, so as to increase the packet delivery ratio, throughput and decrease the average end-to-end delay and overhead. The simulation results also show that the GNDA protocol has good performance when the network is in high density or the traffic is in heavy load.

REFERENCES

[1] Xin Ming Zhang, En Bo Wang, Jing Jing Xia, and Dan Keun Sung, "A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad Hoc Networks" Proc. IEEE Transactions , vol. 12, no. 3, march 2013

[2] J. Kim, Q. Zhang, and D.P. Agrawal, "Probabilistic Broadcasting Based on Coverage Area and Neighbor Confirmation in Mobile Ad Hoc Networks," Proc. IEEE GlobeCom2004.

[3] H. AlAamri, M. Abolhasan, and T. Wysocki, "On Optimising Route Discovery in Absence of Previous Route Information in MANETs," Proc. IEEE Vehicular Technology Conf. (VTC), pp. 1-5, 2009.

[4] X. Wu, H.R. Sadjadpour, and J.J. Garcia-Luna-Aceves, "Routing Overhead as a Function of Node Mobility: Modeling Framework and Implications on Proactive Routing," Proc. IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems (MASS '07), pp. 1-9, 2007.

[5] J.D. Abdulai, M. Ould-Khaoua, L.M. Mackenzie, and A. Mohammed, "Neighbour Coverage: A Dynamic Probabilistic Route Discovery for Mobile Ad Hoc Networks,"Proc. Int'l Symp. Performance Evaluation of Computer and Telecomm. Systems (SPECTS '08), pp. 165-172, 2008.

[6] Z. Haas, J.Y. Halpern, and L. Li, "Gossip-Based Ad Hoc Routing," Proc. IEEE INFOCOM, vol. 21, pp. 1707-1716, 2002

[7] F. Stann, J. Heidemann, R. Shroff, and M.Z. Murtaza, "RBP: Robust Broadcast Propagation in Wireless Networks,"Proc. Int'l Conf. Embedded Networked Sensor Systems (SenSys '06),pp. 85-98, 2006.

[8] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," EUROCRYPT: Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques, pp. 272-293, 2003.

[9] A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, "A Survey of Key Management in Ad Hoc Networks," IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.

[10] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," EUROCRYPT: Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques, pp. 272-293, 2003.

[11] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

