International Journal of Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.05,Issue.44
November-2016,
Pages:9180-9184

www.ijsetr.com

# A Survey on Enhancing the Route Reliability and Stability in Heterogeneous Multihop Wireless Networks

**B. SATEESH KUMAR[1], V. UMARANI[2], K. TANMAI[3]**

[1]Asst Prof, Dept of CSE, JNTUH College of Engineering, Jagitial, Karimnagar, TS, India, E-mail: sateeshbkumar@gmail.com.
[2]Asst Prof, Dept of CSE, School of Information Technology, JNTUH, Hyderabad, TS, India, E-mail: umarani@jntuh.ac.in.
[3]PG Scholar, Dept of CSE, School of Information Technology, JNTUH, Hyderabad, TS, India, E-mail: tanmai4a1@gmail.com.

**Abstract:** In multi-hop wireless networks more than one wireless nodes are used to offer coverage to a large region by way of forwarding and receiving data wirelessly among the nodes. Along with multimedia data transmission and information sharing ,Heterogeneous Multihop Wireless Networks can put into effect many beneficial applications. In HMWNs, a route is damaged when an intermediate node out of range of its neighbours in the routing direction. In addition, a few nodes can also damage routes as they do not have enough energy to transfer the packets of the source node and keep the routes connected. It may also endanger the reliability of information transmission and the network's overall performance is degraded in phrases of packet delivery ratio. In this project, we advise E-star for organizing reliable and strong routes in heterogeneous multihop wireless networks. E-star puts together payment and believe structures with a electricity-aware and trust-based routing protocol. The nodes that relay others' packets are rewarded by payment system and who send packets are charged. The trust system evaluates the nodes' reliability and competence in relaying packets in phrases of multi dimensional trust values. The trust values are connected to the public-key certificate of the node for use in making routing decisions. We broaden two routing protocols to direct traffic through the ones relatively-relied on nodes having enough strength to minimize the probability of breaking the path. Thus E-star can stimulate the nodes to forward packets, and also to report accurate battery power capability and to maintain path stability.

**Keywords:** TP, HMWNs, SRR and BAR.

## I. INTRODUCTION

Routing process in ad-hoc wireless networks is an important area of research studies for many years. Plenty of the unique work within the vicinity became motivated by way of mobile software environments, inclusive of battlefield adhoc networks. In those environments the main focus is to offer scalable routing. These days, exciting industrial packages of multi-hop wireless networks are evolved these days. One instance of such packages is community networks(wireless).Individual transfer's performance or enhancing the network capacity are dealed by the routing algorithms in those networks, rather than dealing with mobility or minimizing energy utilization. The reduction in overall ability because of interference between the multiple simultaneous transformations is one of the foremost problems dealing with such networks. Heterogeneous Multihop Wireless Networks can put into effect many beneficial applications along with multimedia data transmission and information sharing. However, the assumption is that the nodes are inclined to spend their constrained resources, such as community bandwidth and battery power. Drawbacks within the present routing protocols such as DSR count on that the network nodes are willing to relay packets of other nodes. In disaster recovery this expectation holds good as under single authority.

This cannot be preserved in civilian applications as the nodes aim to maximize their advantages, because their involvement consumes their valuable sources which includes bandwidth, electricity, and computing strength without any advantages. In many civilian applications, the selfish nodes will not like to cooperate without sufficient incentive, and to relay their packets they employ the cooperative nodes, which has terrible effect on the community equity and overall performance. Equity trouble arises when a selfish node takes benefit from the cooperative nodes without contributing to them. The network performance is significantly degraded because of this selfish behavior ensuing in failure of the multi-hop communication. Further, a few nodes might also break routes due to the fact they do no longer have sufficient power to relay the source nodes' packets and hold the routes linked. Due to this uncertainty within the nodes' behavior, randomly deciding on the nodes that forward packets will reduce the routes' balance. To overcome those drawbacks, in this paper we put forward E-STAR to establish reliable and stable routes in HMWNs. This proposed system utilizes the trust and payment system. The payment system makes use of credits to reward the nodes that relay packets and rate the nodes that send packets. The trust system is important to examine the nodes' trustworthiness and the reliability within the relaying packets. A node's trust fee is described because

it is the degree of notion about the node's behavior. From the previous behavior of the node the trust values are calculated and are used to expect their destiny behavior.

The heterogeneous Multi-hop wireless Networks has cellular nodes and offline trusted party whose public key is regarded to all the nodes. The cellular nodes have special hardware and energy abilities. Each and every node has a completely unique identification and public/personal key pair with a limited time certificates issued with the aid of TP. without a valid certificate, the node cannot talk nor act as an intermediate node. TP keeps the node's credit score money owed and accepts as true with values. Every node contacts TP to submit the fee reports and TP updates the concerned node's fee bills and trust values. After updation of the trust values the routing establishment process is done through SRR and BAR. SRR can realize a shortest and reliable path and it avoids the low trustworthy nodes. Whereas BAR can realize the foremost reliable one. Thus the E-STAR has three main modules. In Data Transmission module, the source send messages to destination node. In Update Credit-Account and Trust Values module, TP determines the rewards and charges of the nodes and also updates trust values of the nodes. Finally, in Route Establishment , stable communication routes are established by the energy-aware and trust-based routing protocol.

## II. RELATED WORK

**[1] Secure Anonymous Communication Protocol for Wireless Sensor Network**

In wireless sensor networks while communicating data, maintaining anonymity is important due security concerns. Among sensor nodes anonymous communication is very important as the sensor nodes, either being a base station or source node, want to cover up their identities. Existing anonymity schemes either suffer from many overheads such as complex computation, more usage of memory and cannot find the complete anonymities. The existing system presents an Secure Anonymity communication protocol (SACP) for wireless networks. It can realize anonymities completely and offers overheads with respect to communication costs, computation and storage. The proposed system performs the task of source, destination and anonymity of intermediate node using the proposed algorithm. To maintain the source and destination anonymity, in our approach the packet is encrypted by the source using destination's public key and employ a changing virtual destination. In wireless sensor networks, anonymity of sensor nodes can prevent attacker from identifying originator node that originates the message and also avoids from capturing main nodes like source node and base station nodes. Three types of anonymities are presented in this paper: sender node anonymity, data communication association anonymity and base station anonymity and is using hash function requiring little computation and symmetric cryptography.

**[2] A Survey on Various Manet Routing Protocols Based on Anonymous Communication**

Mobile Ad hoc Networks (MANETs) are a Wireless, self configurable and infrastructure independent networks. MANETs have grown to be a attracting and challenging choice for disaster – response and millitary operations. As such networks permits exchange of messages on a network without disclosing the identifiers of network to each other or to third parties, anonymous communication is a challenging topic. This type of communications can be revealed by means of traffic analysis. This analysis is an advanced approach and exposes relationships between users of anonymous communication systems. Various protocols for reducing anonymity communication in MANETs are presented by the present servey. Each surveyed method is very efficient in terms of its performance metrics and resilient to various attacks. The advantages and disadvantages of each method in various aspects is shown in this servey. The efficiency of those methods can be measured in terms of computational time, computational complexity, overhead, power consumption and throughput respectively.

**[3] Selective Acknowledgement Scheme that reduce misbehavior of Routing in Mobile Ad Hoc Network**

In Mobile Ad Hoc Networks (MANETs),cooperation among the nodes is very important . In a self-organization way, each node helps the other to perform network functions. However, some selfish nodes may oppose to cooperate with others to avoid consumption of their battery power and other resources. This paper proposes selective acknowledgment (SACK), acknowledgment scheme that is end to end. It can be easily attached on top of all source routing protocol. The selfish nodes of network are prevented to improve the performance. This paper presents preliminary evaluation and additional SACK scheme information. This paper provides a frame work in detecting misbehaving nodes and isolation of such nodes from routing process in MANETs. It can be combined on top of any source routing protocol such as DSR. A comprehensive analysis of routing misbehavior was made to develop a security module that would meet the network security goal. Currently we are working on its simulation in ns-2 simulator [15] to show the results and effectiveness of our solution on DSR routing protocol. To address other attacks such as gray hole and black hole attacks in MANETs, similar approaches can also be integrated to these source routing algorithms.

**[4] LogitTrust: A Logit Regression-based Trust Model for Mobile Ad Hoc Networks**

MANETS have many applications in different environments. To compete with malicious nodes, trust is an effective mechanism. There are several obstacles like dynamic environments, limited observations and authority that degrade accuracy of trust. A model is proposed by this paper and is named as log it trust .This is for service-oriented MANETs to model dynamic trust , where a node can be a provider (SP) or a requester (SR) of service . Based on Bayesian Inference the traditional approaches are outperformed by logit trust for trust accuracy and reciliance against attack, when given the same amount of limited observations and false positive rate maintained low. This

paper proposed a novel regression based trust model, LogitTrust which evaluates SP trustworthiness for executing and delivering a service in service-oriented MANET environments. It assesses each SP in terms of its service patterns ,response to environmental and operational changes. The net effect is that we are able to learn and then predict its behavior, instead of judging its trustworthiness just from recommendations or local observations received by a SR. Our simulation results show that with the Bayesian Inference , LogitTrust overcomes traditional approaches believing the discounting in terms of the rate of unsatisfactory service received, rate of receiving a satisfactory service and the rate of satisfactory service missed in the presence of socially selfish nodes per- forming false recommendation attacks, when given the same amount of recommendations and observations as input.

**[5] Performance of Swarm Based Intrusion Detection System Under Different Mobility Conditions in MANET**

It is difficult to detect the intrusion in mobile ad hoc network (MANET),due to MANET features such as mobility, limited transmission range and dynamic topology. In this paper, three (Swarm based Intrusion detection)SBDTs are created namely Sbdtlow-Mobility, Sbdtmedium- mobility and SBDTHIGH-MOBILITY. In the SBDTs, nodes with more residual energy, bandwidth and trust value are selected by swarm agents, as active nodes. The active nodes collect the trust values from its neighbouring nodes. As per the trust thresholds the active nodes keep changing. After the exchange of trust values some nodes are marked by active nodes as malicious nodes if it finds the node below minimum trust threshold. When an alert message is received by source rabout the malicious node,it deploys a defense technique to remove that node . Simulation results shows that the SBDT-HIGH-MOBILITY is producing better results while varying the nodes and SBDTLOWMOBILITY produce good results when varyin attackers. This shows that the major role in this mechanism is played by the mobility condition.

**[6] The Role of Trust Management in Distributed Systems Security**

Today's Internet requires robust and powerful tools for handling security, which the existing mechanisms cannot provide. These mechanisms which increase the Internet's programmability come from the development and deployment of systems. This "improved flexibility due to programability" trend is increasing with the invent of Mobile Agents and Active Networking. To overcome the limitations a trust based system is improved. Trust-management engines prevents the necessity to resolve "identities" in an authorization decision. Instead, they express restrictions and privileges . This increases expressibility and flexibility and also for security mechanism's standardization. This approach also includes proofs with transactions that comply local policies and system architectures. This encourages administrators and developers to carefully consider an application's security policy and to explicitly specify it. In this paper,we analyze the limitations of existing systems. It introduces the trust management concepts that explain its basic principles, and explains some trust-management engines which are existing, including Key Note and Policy Maker.

**[7] An Acknowledgement-Based Approach to Detect Misbehaviour of routing in MANETS**

The Routing misbehavior in MANETs (Mobile Ad Hoc Networks) is considered by us here. The assumption is that all the intermediate nodes are cooperative. But, there may be existence of node misbehaviors due to the open structure. One of the misbehavior in routing is that few nodes will take part in the maintenance processes and route discovery but refuse to relay the data packets. Serving as an add-on technique this paper proposes the 2ACK scheme that mitigates their effect and to detect misbehavior in routing. In the routing path's opposite direction two-hop acknowledgment packets are sent and this is the basic idea . In this scheme only some of the packets are acknowledged in order to minimize extra overhead in routing. The proposed system detects malicious links in the Network as it is a simulation of the algorithm. It implements the 2ACK scheme to detect misbehavior . This technique that mitigates the routing effects. It also finds misbehavior of routing by making use of a new acknowledgment packet, called 2ACK packet. In the direction opposite to the data traffic route, a fixed route of two hops is assigned(three nodes N1, N2, N3).

**[8] MODSPIRITE: A Solution Based on Credit to Improve Cooperation of Node in an Ad-hoc Network**

Cooperation among nodes is an important factor in ad-hoc network to transmit the data successfully among the nodes. The assumption is that the intermediate nodes will cooperate in communication. However, because of limited bandwidth, energy and computational resources, sometimes a node may be selfish and it do not like to waste its resources. These nodes are unwilling to the packets of others' .The existing credit based and reputation based systems are reviewed/revised in this paper. MODSPIRIT, a credit based solution is proposed and is a modification of SPIRITE system. Using mechanism of neighbor monitoring and by giving incentives to intermediate nodes, this system identifies and enforces the cooperation among selfish nodes. The sender node loose the credit in relay of data and hence to forward the data in future it has very less or no credit, which is one of the SPIRITE system's limitations. The MODSPIRITE reduces sender' overhead for upto 25% and it also punishes selfish nodes.

**[9] Attacker free and Trusted System based on credits of nodes For Multihop Wireless Networks**

A new system called TACS is proposed, a trusted and attacker free credit based scheme for wireless networks(TACS). It is used to stimulate node co-operation, regulate packet transmission and avoid packet drop. After the completion of communication, a report is submited to the trusted party and stores a temporarily undeniable token called evidences. The report is verified by the trusted party. It also removes cheating node from the system. To all the nodes in the new system a trust value is assigned after

removing all the attackers. This will improve the security of the system and it has low processing overhead and communication overhead. This paper is based on credit based system for attacker free and trusted credit systems for wireless networks. Different techniques were conducted by many researchers to propose different types of payment schemes because of the nature of limited resources on wireless nodes. All the schemes have some advantages and some disadvantages. To avoid selfish nodes in the network and to enforce node co-operation and here we describe different payment scheme. A good credit based scheme requires less overhead and should be secure. It also secures the data transmission in the network.

**[10] ESIP: Incentive secure Protocol with Less Use of Public-Key Cryptography for Multi-hop Wireless Networks**

In multihop wireless networks, some nodes are very selfish and do not forward the packets of neighbour nodes' but for transferring their packets, they make use of the cooperative nodes .The network performance and fairness are degraded because of this. Hence to stimulate the selfish nodes' cooperation, the Incentive protocols use credits. But to secure the payment, the existing protocols depends on the public-key operations that are of heavy-weight. This paper proposes secure cooperation incentive protocol .Only for the first packet in a series public-key operations are used and for the next packets light-weight hashing operations are used. Hence packet series's overhead converges/combines with hashing operations. The proposed protocol is demonstrated as secure by the performance evaluation and security analysis. The nodes' operations are dominated by the efficient hashing operations. This makes the overhead in comparible to incentive protocols that are public key based. For a series of two packets, DSA and RSA based protocols have higher cryptographic delay and energy than ESIP, and for a series of 13 packets, ESIP requires around 10% of the energy and cryptographic delay in RSA and DSA based protocols. Compared to the very high probability protocols RSA and DSA ,ESIP has less overhead e.g., the data packet overhead in ESIP is 37% and 70% of that in the RSA and DSA based protocol in a 10 packet series, respectively. To encourage the rational packet droppers to participate in the communication, in this paper virtual currency is implemented for the multi-hop wireless network.

However, the irrational packet droppers, e.g. cooperative nodes spend their resources like credits, energy, bandwidth, etc to degrade the network's performance and then dropping the packets intentionally. Statistical methods are required to identify the attackers who drop the packets more than the normal rate as the sessions may be normally broken, e.g., due to mobility, or due to malicious actions intentionally. The receipt format in ESIP can reveal the node that breaks the route. So in our future work, we can extend this work to take the irrational packet droppers in to consideration. The trusted party updates the receipts to make a good system. To avoid identifying honest nodes wrongly as irrational packet droppers and to identify the attackers in short time to reduce their harm,a standard system is designed .

**[11] Payment Schemes for Securing Multihop Wireless Networks: A Survey**

In a multi-hop wireless networks, a packet is traversed in various wireless links to meet the destination. Unlike mobile adhoc networks, nodes in multi-hop wireless network are fixed. These networks enhances the spectral efficiency, throughput of network, enlarges the area with less transmit power and can be deployed at less cost. But these networks suffers from various attacks. The selfish nodes in these networks, do not forward but they depend on cooperative nodes to forward their packets. To find selfish nodes many schemes are proposed in the paper. In receipt-based payment scheme, accounting center organizes and accumulates the t account of the nodes. For updation of credit accounts, each node in the network submits to the accounting center or trusted party, the proofs about forwarding the packets. But the drawback in this method is computational complexity and high communication overhead. This paper proposed various payment schemes and analyzed their performance. This paper proposes many payment schemes for security enhancement with low computation overhead in multi-hop wireless networks. One of the methods is Receipt based method. In this method the accounting center organizes and accumulates the credit account of the nodes. But this has high overhead. In the tamperproof-device (TPD)-based payment scheme, in every node a tamper-proof-device is installed for securing the operation and organize the credit account. But the drawback is that during the communication time, if the nodes do not have adequate credits they cannot communicate. Thus an effective method is proposed to improve the security with less complexity for wireless networks and less processing overhead.

## III. CONCLUSION

This project proposed E-STAR based mostly Anonymous Location-based economical Routing protocol that uses trust/payment systems with energy-aware and trust-based routing protocol to determine reliable and secure routes in HMWNs. E-STAR stimulates the nodes not solely to forward packets of other nodes, but additionally to keep up the route stability. It additionally punishes the nodes that report wrong energy capability by minimizing their likelihood to be chosen by the routing protocol. SRR and BAR routing protocols are proposed and are evaluated in terms of route stability and overhead. Our protocols will make advised routing choices by considering multiple factors, together with the route length, the route reliableness based mostly on the nodes' past behavior, and also the route period of time supported the nodes' energy capability.

## IV. REFERENCES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

[2] C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer

Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, Jan. 2007.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom'00, pp. 255-265, Aug. 2000.

[4] X. Li, Z. Li, M. Stojmenovic, V. Narasimhan, and A. Nayak, "Autoregressive Trust Management in Wireless Ad Hoc Networks," Ad Hoc & Sensor Wireless Networks, vol. 16, no. 1-3, pp. 229-242, 2012.

[5] G. Indirania and K. Selvakumara, "A Swarm- Based Efficient Distributed Intrusion Detection System for Mobile Ad Hoc Networks (MANET)," Int'l J. Parallel, Emergent and Distributed Systems, vol. 29, pp. 90-103, 2014.

[6] K. Liu, J. Deng, and K. Balakrishnan, "An Acknowledgement Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536- 550, May 2007.

[7] S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, vol. 3, pp. 1987-1997, Mar./Apr. 2003.

[8] M. Mahmoud and X. Shen, "PIS: A Practical Incentive System For Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

[9] M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997- 1010, July 2011.