Volume 5, Issue 7, July 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Deep Analysis: Highly Robust Fault Tolerant Secure Optimized Energy Ad-hoc Networks Methodologies for Mobile Nodes

Nisha Chaudhary[1], Er Shiv Kumar Goel[2], Nitin Goel[3]

[1, 2] Department of ECE, KITM, India

[3] Patent Analyst, MSPE, Noida, India

Abstract*— Mobile ad hoc network especially follows multi-hopping mechanism for routing to make a path from source to destination. If we have a sound and solid routing path that would be efficient, reliable and adaptable to the different scenarios of network too by following the next hop mechanism and also should be the farthest node within the cluster then we could achieve better performance by the network. Mobile ad hoc networks (MANETs) are a kind of network that has no centralized body and in order to communicate with the nodes it has no fixed topology. Also it is difficult to find the route from source to destination in MANETs, because of its arbitrary mobility of nodes and in general MANETs works on multi-hop environment to select a route from source to destination. In this paper we will discuss the various exiting approaches which give highly robust energy efficient routing protocols for MANETs. We will discuss the pros and cons of existing protocols, which help researchers to excel their innovation in the field of highly optimized energy efficient network.

***Keywords*— Energy Efficient, MANETs, Secure, Optimized, Routing, Fault Tolerant**

I. INTRODUCTION

Mobile ad hoc network (manet) is an appealing technology that has attracted lots of research efforts. ad hoc networks are temporary networks with a dynamic topology which doesn't have any established infrastructure or centralized administration. mobile ad hoc networks (manets) are dynamically configure, multi-hop wireless networks with varying topology. mobile nodes in such networks are continuously associated or disassociated with each other, according to their topological arrangements. thus, the network topology varies with time due to the ataxic locomotion of the participating nodes. In recent years the concern over the security of computer networks has been widely discussed and popularized. the discussion has, however, typically involved only static and wired networking while the mobile or ad-hoc networking issues have not been handled extensively. the emergence of such new networking approaches sets new challenges even for the fundamentals of routing since the mobile ad-hoc networks ,(manet) are significantly different from the wired networks.[6,7,8]

Mobile ad hoc networks are such kind of network that works under dynamic routing with mulihopping mechanism and have no centralized body to govern the network under which the network has to communicate. apparently it's crucial to work with such kind of network because of the absence of base stations/routers. in manets nodes itself have capability to act as base station/router and every node may function as a router and forward packets through routing paths. Co-operation among nodes during path discovery and packet relaying is of primary concern and should be supported for correct functioning of the network. Communication in a manet occurs in a discrete and disperse environment with no centralized management which arises a main issue in manet that is the breakage of link at certain moment and re-generation of link at certain state. In order to work with manets we have some predefined routing strategies through which we can pursue our communication i.e. active routing (on demand), proactive routing (table driven). rest of these there is one more routing strategy known as preemptive routing (works on the bases of signal strength and age of path) all these strategies have their own pros and cons. all these protocols have some excellent features if we intermingle all these features especially give more emphasis on signal strength that acts as threshold and we could lead towards a website.

II. RELATED WORK

Along with these routing strategies, if we could improve the path election/selection process on the bases of the parameters and constraints that are directly related to the given network definitely we would have a sound, efficient and adaptable network. In this paper we will discuss the various exiting approaches which give highly robust energy efficient routing protocols for MANETs. We will discuss the pros and cons of existing protocols, which help researchers to excel their innovation in the field of highly optimized energy efficient network.

To overcome the adverse elements in the network, Sajal K. Das et al [9], proposed a trust based model where a comprehensive reputation model is designed integrating direct and indirect observation of nodes. Based on these observations the future forwarding behavior of a node is predicted. The framework is based on the Positive Feedback Message (PFM) that is designed as the evidence of the forwarding behaviour of the node. But the paper does not address certain issues like the impact of mobility and direction of a node on routing. Further the fact that from indirect observation a node might be deceived with wrong values causing its own trust levels of various nodes to fall.

Wang Bo et al [10] formulated a trust based minimum cost opportunistic routing for adhoc networks. In order to alleviate malicious behavior, the concept of trust built a simple model that evaluates the neighbors and their forwarding behavior. The paper also applied this model to opportunistic routing for adhoc networks. Though the simulation results proved the work to be efficient the self trusting principle used in the work causes delay. Further most of the evaluation is based on assumptions and theoretical calculations.

Jieying Zhou, et al [11] presented SRSN: Secure Routing based on Sequence Number for MANETs to defend against black hole attack. This paper proposed a new method SRSN (Secure Routing based on Sequence Number) based on which the strict increment of sequence number of RREQ packet combined with reliable end to end acknowledgement to detect false route information. SRSN detects bogus RREQ forged by malicious node through the discontinuity of sequence number of RREQ packet combined with the normal process of data transmission.

Jason Lebrun, et al [12] compared five different opportunistic forwarding schemes which vary in their overhead, their success rate, and the amount of knowledge about neighboring nodes that they require. The design goal is to deliver data successfully to static destination with minimal delay. Qualnet is used to simulate and compare five different algorithms: No talk, Broadcast, Location based, MoVe, MoVe look-ahead. The Location based algorithm uses relative position between vehicles and destination to make a forwarding decision, while MoVe vector and MoVe look- ahead take into account relative velocities of the vehicles.

III. VARIOUS EXISTING SCHEMES RELATED TO ENERGY EFFICIENT ROUTING METHODOLOGY WITH PROS AND CONS

1) SDSR: A Secure on-Demand Routing Protocol for MANETS: Secured data transmission in Mobile Ad-hoc Networks (MANET) are most recent research issues for ensuring full applicability of deploying MANETs in wide range of applications, including strategic as well as nonstrategic. On-demand routing protocols for Mobile Adhoc Networks (MANET) include Dynamic Source Routing (DSR), which is capable of discovering multiple routes. Secure Dynamic Source Routing Protocol (SDSR) on the other hand provides mechanism for secured route discovery, even under adversarial conditions. Moreover, SDSR uses a very efficient broadcast authentication mechanism which does not require any clock synchronization and facilitates instant authentication. Here we uses NS2 simulator and several different simulation results show that performance of SDSR is improved when compared to Ariadne and DSR. In this method they introduced a secure routing protocol SDSR based on DSR, which uses a broadcast authentication scheme which does not depends on clock synchronization for secure infrastructure in MANET. From the above result comparisons it is concluded that performance for packet delivery ratio, average latency and Throughput is improved in SDSR as compare to DSR and Ariadne in the presence of presence of tunneling attacks. In future we are going to implement SDSR in various attacks and test the performance.

2) S-ALERT: Secure Anonymous Location-Based Efficient Routing protocol: In Mobile Ad Hoc Network (MANET), some routing protocols are proposed to hide the identity of node from outside entities that can observe data traffic which can be disastrous in military operations. However, existing protocols which provide full anonymity of source node, destination node and routes are vulnerable to malicious activites. The anonymous protocols hide the identity of the malicious node and enhance the possibility of Black Hole Attack. In order to provide anonymity without compromising the security, we have extended Anonymous Location Based Efficient Routing Protocol(ALERT) to make it secure. The secure version is namedas Secure Anonymous Location Based Efficient Routing protocol (S-ALERT).S-ALERT uses Suspect Detection algorithm to choose the nodes in a route which provide unperceivable route. If there is existence of a Black Hole it actually sends a false RREP packet and advertises itself as the shortest route found. The proposed scheme avoid the black hole problem, and also prevent the network from further malicious behavior. Through simulation results it has been shown that proposed method can effectively detect and provide protection from black hole attack. S-ALERT routing efficiency is also better than existing protocols. In order to provide high security on low cost we proposed S-ALERT which not only hides the identity of nodes but also secure the network from malicious activities. The tradeoff between security and anonymity has been maintained. The main motive is to make the nodes anonymous without compromising the cost and security. They have used Intrusion Detection System which works on probability of node being malicious and when the probability increases the Intrusion Prevention System discard that particular node from the network. Through experiment result it has been shown that introducing security in ALERT does not degrade the performance of the network. Through experiment result it has been shown that introducing security in ALERT does not degrade the performance of the network. S-ALERT is able to provide security from black hole attack in the network along with anonymity

3)Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs: Mobile Ad Hoc Networks (MANETs) are collections of mobile nodes that can communicate with one another using multihop wireless links. MANETs are often deployed in the environments, where there is no fixed infrastructure and centralized management. The nodes of mobile ad hoc networks are susceptible to compromise. In such a scenario, designing an efficient, trustworthy and secure routing protocol has been a major challenge over the last many years. In this paper, we propose a Trust Based Secure On Demand Routing Protocol called "TSDRP". Ad hoc On-demand Distance Vector (AODV) routing protocol has been modified to implement TSDRP for making it secure to thwart attacks like Blackhole attack and DoS attack. To evaluate the performances, we have considered Packet Delivery Fraction (PDF), Average Throughput (AT) and Normalized Routing Load (NRL). Proposed TSDRP is a robust, secure on-demand routing protocol enables the secure route discovery and its maintenance in MANETs. TSDRP protocol is capable of delivering packets to the destinations even in the presence of increasing number of malicious node and increasing number of traffic connections in the MANETs. They have compared performance of TSDRP with that of AODV with respect to different performance metrics. Simulation has been carried out under various scenarios and after observation of performance analysis, it can be concluded that in case of black hole attack and DoS attack TSDRP has performed very well in almost all parameters: PDF, AT and NRL as compared to AODV.

4) *Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET:*In this paper, we propose a solution for detecting and avoiding black hole attacks (both single and cooperative) and ensuring secure packet transmission along with efficient resource utilization of mobile hosts at the same time. According to our proposal, evaluation of trust of every node in the network is based on parameters such as stability of a node defined by its mobility and pause time, remaining battery power etc. This trust of a node forms the basis of selection of the most reliable route for transmission. The simulation results show that our solution provides good performance in terms of throughput, secure routing, and efficient resource utilization. Black-hole attack is one of the most severe routing attacks that is often encountered in MANET. In this attack, a malicious node sends fake RREP to a source node that initiates route discovery, and consequently deprives data packets from the source node. Many researchers have proposed different solutions for preventing black-hole attack. In MANET network topology changes continuously. In this paper, they have analyzed black-hole attack and proposed a solution based on trust of the individual nodes to detect and prevent black-hole attack in MANET. Trust has been calculated based on a few important parameters of a node such as rank, mobility, available battery power, etc. Experimental results show that proposed solution gives good performance in terms of high packet delivery ratio and high throughput as well as efficient energy utilization and also effective black-hole attack detection with minimal number of packet drop.

5) Efficient And Secure Trust Based Ad Hoc Routing In MANET: A mobile ad-hoc network (MANET)[1] is a self configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. The use of wireless ad hoc networks also introduces additional security challenges that have to be dealt with. Efficient Trust based Ad Hoc Routing (ETAR) is an algorithm to provide secure routing in ad hoc mobile networks. We propose this scheme that has been drawn from a network of friends in real life scenarios. The algorithm works by sending challenges and sharing friend Lists to provide a list of trusted nodes to the source node through which data transmission finally takes place. The nodes in the friend list are rated on the basis of the amount of data transmission they accomplish and their friendship with other nodes in the network. The account of friendship of a node with other nodes in the network is obtained through the Share Your Friends process which is a periodic event in the network. As a result of this scheme of operation, the network is able to effectively [2]isolate the malicious nodes which are left with no role to play in the ad hoc network. After a logical analysis and extensive simulation of the ETAR algorithm under different scenarios, we come to the conclusion that it offers robust scheme to afford security for mobile ad hoc networks and performs better than the trust based protocols from which it was compared.

6) Provisioning secure on-demand routing protocol in Mobile ad hoc network: Mobile ad-hoc network (MANET) has been a leading technology for ubiquitous networking since a decade, in which an ad-hoc routing is one of its fundamental components. Due to a number of inevitable challenges in MANETs, especially a problem of secure routing is longstanding, many researchers have extensively studied and developed various techniques to secure on-demand routing protocols in MANETs. However, many open issues remain in secure on-demand routing for MANETs. In this paper, we propose a lightweight and efficient security mechanism for ondemandsource routing protocol including DSR in MANETs. The proposed scheme provides key generation by using a self certified public keying technique as well as ensures secure route discovery by employing Schnorr digital signature and multi-signatures scheme. We provide security analysis of the proposed scheme. It can be seen that the proposed approach ismore secure than the existing schemes. We also evaluated the proposed approach using computer simulation and comparedits performance to that of SRP. The results show that the proposed mechanism is better than SRP. In this paper, they provide a light-weight and efficient security framework for on-demand source routing in the wireless ad hoc network. The proposed scheme utilizes a self-certified public keying technique for lightweight and efficient key generation and deploys Schnorr digital signature scheme and a multi-signature scheme for efficient and secure route discovery. We have analyzed its robustness to various attacks and the simulation results show that it is robust against misbehaving activities.

7) Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs: Decentralized node admission is an essential and fundamental security service in mobile ad hoc networks (MANETs). It is needed to securely cope with dynamic membership and topology as well as to bootstrap other important security primitives (such as key management) and services (such as secure routing) without the assistance of any centralized trusted authority. An ideal admission technique must involve minimal interaction among MANET nodes, since connectivity can be unstable. Also, since MANETs are often composed of weak or resource-limited devices, admission must be efficient in terms of computation and communication. Most previously proposed admission protocols are prohibitively expensive and require heavy interaction among MANET nodes. In this paper, they focus on a common type of MANET that is formed on a temporary basis, and present a secure, efficient, and a fully noninteractive admission technique geared for this type of a network. Our admission protocol is based on secret sharing techniquesusing bivariate polynomials. They also present a new scheme that allows any pair of MANET nodes to efficiently establish an on-the-flysecure communication channel.

IV. CONCLUSION

Mobile ad hoc networks are such kind of network that works under dynamic routing with mulihopping mechanism and have no centralized body to govern the network under which the network has to communicate. Apparently it's crucial to work with such kind of network because of the absence of base stations/routers. In MANETs nodes itself have capability to act as base station/router and every node may function as a router and forward packets through routing paths. Co-operation among nodes during path discovery and packet relaying is of primary concern and should be supported for correct functioning of the network. Communication in a MANET occurs in a discrete and disperse environment with no centralized management which arises a main issue in MANET that is the breakage of link at certain moment and re-generation of link at certain state. In order to work with MANETs Based on predefined routing strategies through which we can pursue our communication i.e. active routing (on demand), proactive routing (table driven). Rest of these there is one more routing strategy known as preemptive routing (works on the bases of signal strength and age of path) all these strategies have their own pros and cons. All these protocols have some excellent features if we intermingle all these features especially give more emphasis on signal strength that acts as threshold and we could lead towards a routing path that is highly efficient in terms of power consumption too.

REFERENCES

[1] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and LixiaZhanng, “Security on Mobile Ad Hoc Networks: Challenges and Solutions” 1536-1284/04/IEEE Wireless Communications Feb., 2004.Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[2] C.Siva Ram Murthy & B.S Manoj, “Mobile Ad Hoc Networks- Architectures & Protocols”, Pearson Education, New Delhi, 2004..

[3] Priyanka, Komal Kumar Bhatia, Ajay Jangra “FRENSA: Farthest, Reliable and Efficient Node Selection Algorithm for Mobile Ad-hoc Networks (MANETs)" in IJCST International Journal of computer Science and Technology Vol. 1 Issue 2 December 2010

[4] Alessandro Mei, JulindaStefa, “Routing in Outer Space: Fair Traffic Load in Multi-Hop Wireless Networks” MobiHoc’08, May 26–30, 2008, Hong Kong SAR, China. Copyright 2008 ACM 978-1-60558-073-9/08/05

[5] Nikos Komninos, Dimitris Vergados, Christos Douligeris “Detecting unauthorized and compromised nodes in mobile ad hoc networks” see front matter _ 2005 Elsevier B.V. All rights reserved. doi:10.1016/j.adhoc.2005.11.005 www.elsevier.com/locate/adhoc

[6] Sumesh J. Philip, Vishal Anand, “Mobility Aware Path Maintenance in Ad hoc Networks” SAC’09 March 8-12, 2009, Honolulu, Hawaii, U.S.A. Copyright 2009 ACM 978-1-60558-166-8/09/03

[7] GautamChakrabarti, Sandeep Kulkarni, “Load balancing and resource reservation in mobile ad hoc networks” Ad Hoc Networks 4 (2006) 186–203 1570-8705 2004 Elsevier B.V. doi:10.1016/j.adhoc.2004.04.012

[8] Na Li, Sajal K Das, “A trust-based framework for data forwarding in opportunistic networks,” Elsevier Ad Hoc Networks, Vol. 11, no. 4, June 2013, pp 1497–1509.

[9] Wang Boa , Huang Chuanhea , et al, “Trust-based minimum cost opportunistic routing for Ad hoc networks,” Elsevier Journal of Systems and Software, Vol. 84, no. 12, dec 2011, pp 2107–2122.

[10] Jieying Zhou, Junwei Chen and Huiping Hu, “SRSN: Secure Routing based on Sequence Number for MANETs,” IEEE, 2007, pp.1569-1572.

[11] Jason LeBrun, Chen-Nee Chuah, et al, “Knowledge-Based Opportunistic Forwarding in Vehicular Wireless Ad Hoc Networks,” Vehicular Technology Conference, IEEE, 2005, pp. 2289 – 2293.

[12] J-H. Cho, A. Swami, and I-R.Chen, “A Survey on Trust Management for Mobile Ad Hoc Networks,” IEEE Communications Surveys & Tutorials, Vol.13, No. 4, Fourth Quarter 2011.

[13] Shen and L. Zhao, “Alert: An anonymous location-based efficient routing protocol in manets,” IEEE Transactions on Mobile Computing,vol. 12, pp. 1079–1093, June 2013.