ENERGY EFFICIENT AND SECURE ROUTING IN MOBILE AD-HOC NETWORKS- A SURVEY

Poonam Mishra[1], Neelesh Gupta[2]

[1]M.Tech Scholar, [2] HOD, ECE, Truba Institute of Science & TechnologyBhopal, (India)

ABSTRACT

An ad-hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any preexisting network infrastructure or centralized administration. However, due to the absence of central infrastructure the devices in the ad-hoc network can move randomly gives rise to various kind of problems, such as routing and security. The nodes in ad-hoc networks are typically battery powered. The need for energy efficiency in MANETs requires power enhancement features. The mobile ad-hoc networks also suffer from security attacks and privacy issues which dramatically impede their applications. To cope with the attacks, a large variety of intrusion detection techniques have been developed. Recent advances in MANETs have lead to many protocols specifically designed where energy awareness and security is an essential consideration. This paper surveys various approaches pursued for security and energy efficiency for different routing protocols and most of the time AODV provided better results. The proposed methods can also be implemented on DSR routing protocol to provide source routing and it can give better results than AODV routing protocol.

Index Terms: Mobile and Ad-Hoc Network, Routing Protocols AODV, DSR, DSDV Power Aware Routing, Secure Routing.

I. INTRODUCTION

Mobile ad hoc network is wireless, infrastructure less, self organizing network with dynamic topology. Nodes in MANET should have a transmitter/receiver as well as routing/switching capabilities because they act as both host and router. Due to the node mobility frequent topology changes occurs in the network. At a given time, the system can be viewed as a random graph due to the movement of the nodes, their transmitter/receiver coverage patterns, the transmission power levels, and the co-channel interference levels. The network topology may change with time as the nodes move or adjust their transmission and reception parameters. Thus, a MANET has several salient characteristics dynamic topologies, resource constraints, limited physical security, and no infrastructure. The communication between nodes is accomplished via other nodes which are called intermediate or forwarding nodes. So there is a need of a routing procedure between nodes. Routing is used for the data transfer between any two nodes if they are not directly connected. Number of routing algorithms has been proposed for mobile ad-hoc network [1], [2]. There are two basic classes of routing protocols used in the MANET. One is proactive routing protocols which are table driven routing protocols. Another class is reactive routing protocols also known as on-demand routing protocols. The reactive routing protocols create and maintain routes only when needed. Most widely used and efficient reactive routing protocol in MANET is Ad-hoc On-demand Distance Vector (AODV) routing. AODV routing protocol works in two phases, one is Route discovery phase and other is Route maintenance. AODV protocol uses the various control packets like RREQ, RREP, and RERR etc. for route

discovery and route maintenance process. Dynamic source routing (DSR) allows to dynamically discovering a route across multiple network hops to destination. The DSR protocol is composed of Route discovery and Route maintenance mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network. Destination-Sequenced Distance Vector (DSDV) is well known table driven protocol, based on Bellman-Ford routing mechanism. Each node maintains a routing table which contains a list of all possible destination nodes within the network along with the no. of hops required to reach to particular node.

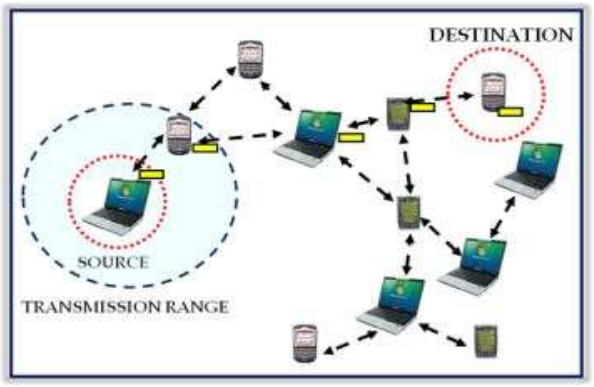

Figure 1: A Typical MANET Network

Security in wireless ad hoc networks has recently gained a momentum and became a primary concern in attempt to provide secure communication in hostile wireless ad hoc environment. Achieving security performances in wireless ad hoc environment is a challenging task because it has inherent vulnerabilities that are not easily preventable. Unlike wired network, any malicious node can attack from all directions and target on any node in MANETs. For instance, in the case of security, the nodes cannot rely on network architecture based defense techniques such as centralized firewalls. Each node thus becomes a point of vulnerability and must assume, by itself, its own security. Battery life and processing power are also major constraints in Ad hoc networks. Mobile ad hoc networks do not have central controller to coordinate the activities of nodes. The nodes can freely move about and organize themselves to form a network. The nodes are limited by their battery power for performing various operations. Routing a packet from source to destination involves an adequate number of intermediate nodes to be traversed. Therefore, battery power of a node should be used efficiently in order to keep the node alive for sufficient time to avoid early exhaustion of a node/network. Energy management is therefore an important concern as it is a "fuel" that keeps the network alive. The greatest challenge manifesting itself in the design of wireless ad-hoc networks is the limited availability of the energy resources. These resources are quite significantly limited in wireless networks than in wired networks. Also the mobility of nodes in MANET influences the energy efficiency and security in the network.

II. RELATED WORK

Routing Optimization in mobile ad hoc networks along with secured transmission is an ever-demanding task. Mobile ad hoc networks are highly dynamic topology natured and hence several routing protocols meet the challenge of link quality, delay and energy conscious routing. This paper [11] proposes a secured link quality, delay and energy conscious routing approach based on ant colony optimization. Based on the estimated link quality, delay and residual energy of the nearby nodes, Adaptive node stability (ANS) mechanism is mathematically modeled to make the routing strategy. SLQDEARP selects the efficient node based on the ANS mechanism and sends the data packets through that node. Ad-hoc security algorithms incorporated for making

the transmission more secured. Ad- Hoc Security Algorithm shortly called as ASA which incorporates secured means of transmission over the ad hoc network has been introduced**.** SLQDEARP is an on-demand unipath routing protocol. The proposed SLQDEARP takes advantage of various features of AODV routing protocol and estimates link quality and also selects the delay and energy aware path towards the destination node**.** The information about the residual energy of the neighbor nodes is stored by every node throughout requesting the other nodes about their residual energies. Theresidual energies at a node can be calculated as- Residual energy = initial energy – consumed energy

The proposed algorithm is an attempt to present a new approach for complex encrypting and decrypting data based on parallel programming in such a way that the new approach can make use of multiple-core processor to achieve higher speed with higher level of security. ADHOC SECURITY ALGORITHM (ASA) is described by a pseudo-code as shown in Fig 2. Simulation results show that SLQDEARP increases delay, energy consumption and packet delivery ratio than AODV and DECRP protocol due to security mechanism incorporated.

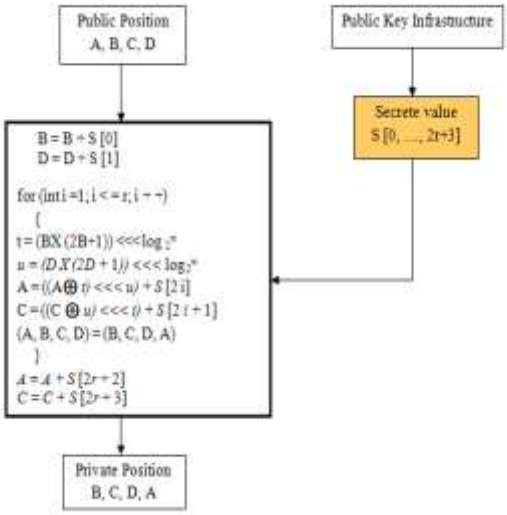

Fig 2: Ad-Hoc Security Algorithm (ASA) Algorithm Structure

Ajay et al. [6] proposed in this paper the technique of implementing biometric with cryptography or intrusion detection system which provides secure alternative for communication over network. This paper critically reviews and investigates the present biometric based security models works for MANETs, and along with security challenges. The resources present in MANET are limited, e.g., battery power MANET is very important resource as it has limited life and are not easily rechargeable. So we have to reduce the energy consumption in MANET by using an efficient routing algorithm for data transmission. Considering the above problems G Varaprasad [9] proposed a paper which presents a new multicast algorithm to increase the lifetime of nodes and network in the mobile ad hoc network. Here, it considers two metrics, namely residual-battery-capacity of the node and relay capacity of the node to do multicasting from the source to a group of destination nodes. If a source node (*S*) wants to send message to the destination node (*D*), then it looks for a route in its routing table. If a valid route is not found, then *S* uses Route Request (RREQ) packet. The node receiving RREQ packet and then sends a Route Reply (RREP) packet to *S*, if it has path to the destination. Otherwise the node broadcasts RREQ packet to the neighbors. After receiving it, *S* selects the shortest path among all and adds this as an entry

into the routing table. If S wants to send multicast packets, then it chooses a node with more residual-battery capacity. If all intermediate nodes have equal residual-battery capacity, then it chooses a node with more relay-capacity. Based on the battery lifetime and relay-capacity of the node, it creates a multicast tree. The key point is that the battery lifetime and relay capacity of the node used to increase the network lifetime. It makes more reliable communication. The proposed model is compared with the existing algorithms such as multicast incremental power, lifetime aware multicast tree, and multicast ad-hoc on demand distance vector protocol and multiple path multicast ad-hoc on demand vector. The simulation results reported in this paper demonstrate that the proposed model improved the network lifetime by 20% on average. Extending network lifetime is accomplished by finding multicast that tends to minimize the variation of remaining energy of all the nodes thus making the MANET network energy efficient. The power-aware multicast protocols tend to create additional control traffics. K. V. Arya et al. [10] proposed two algorithms to improve the energy consumption and security of MANET. The proposed algorithms utilize the dynamic route shortening and local route repair scheme to improve the reliable packet delivery and enhance the route maintenance if route breaks occur due to less remaining energy in the nodes. The path breakage due to the less battery power is reduced by dynamically replacing the nodes with very less power by the nodes having sufficient amount of power. In original AODV when any route breaks then the upstream node sends the Route error (RERR) message to the source node which initiates process to create the new route to provide the further communication. In the proposed work the route is created locally by using those neighboring nodes of the upstream nodes which have the highest energy. By this we can increase the life of the node. Energy weights are assigned to each node as shown in Fig 3 and in case of route break alternate route is selected on the basis of energy weights of nodes as shown in Fig 4.

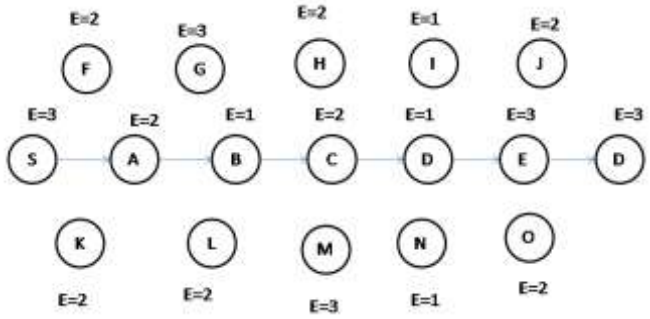

Fig 3: All the Nodes with their Energy Weights

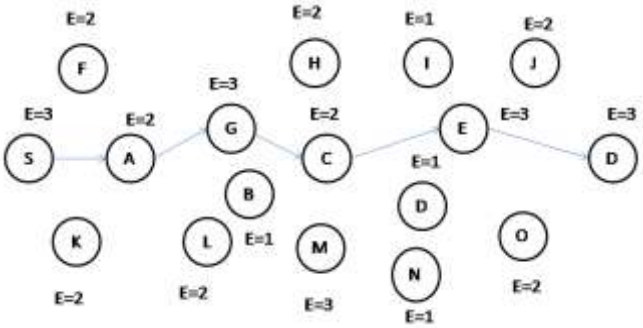

Fig 4: Selection of Alternate Local Route on the Basis of Energy Weights

A distributed algorithm has also been developed to reduce the packet dropping attack in MANET which has been simulated on (NS-2) and demonstrated an increase in packet delivery ratio, throughput while decrease in average

end-to-end delay as compared the basic AODV protocol. The comparison of packet delivery ratio among proposed AODV and AODV with black-hole against various values of pause time is shown in Fig 5 for the network with 100 nodes. We can clearly see from the figure that AODV with security algorithm (AODVS) is producing higher PDR in comparison to the AODV with attack (AODVB). Therefore, the proposed method is more efficient and gives better results in terms of packet delivery.

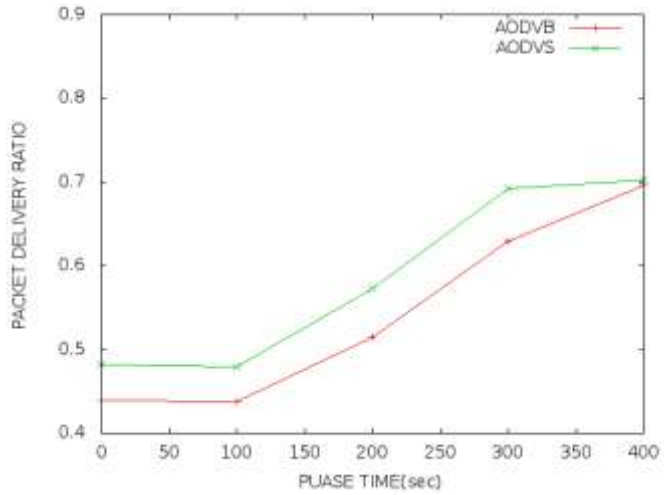

Fig 5: Packet Delivery Ratio Comparison in Security Model for 100 Nodes

Haidar Safa et al. [7] proposed power aware heterogeneous AODV (PHAODV) routing protocol that uses efficiently the energy available in nodes when establishing and maintaining heterogeneous routes in the network. The protocol extends HAODV routing protocol which selects the shortest stable routes composed of nodes equipped with heterogeneous interfaces. HAODV allows heterogeneous nodes in a route regardless of the nodes' underlying technology. The proposed PHAODV assumes that the nodes are enabled with an interoperability model that is responsible for handling the packet conversion from one technology to another. The information acquired by a node about its neighbors through routing messages is stored in the neighbors list with an identification of the interface through which this information was acquired. The interface identifier is used as an indication of the signal type between neighbor nodes in future communication. This information is not appended to the packets' headers and is kept in the routing tables to avoid any unnecessary increase in packet size. The work in [8] provides energy oriented power controlled mechanism to efficiently utilize the energy reserves and increase the network lifetime. The central idea is to select a Lead Node that will centrally manage the energy levels of the various nodes in an Energy Table (ET). The route is selected based on per node instead of per flow to avoid the drainage of a particular network node or path.

A preventive approach based on a cryptographic mechanism and a reactive approach to detect the anomalous and malicious behavior of nodes is considered in [3]. An extension of secure AODV (SAODV) to offer intrusion detection mechanism (IDM) and trust based mechanism (TBM) to promote the collaboration of the cooperating node and penalize the selfish nodes are proposed. SAODV with IDM and TBM proves to outperform SAODV when internal attacks are effectuated and the incentive cooperation mechanism and IDM permit reduction of the impact of malicious nodes determining better performance. In [4] an energy efficient route discovery process for AODV based on expanding ring search technique (ERS) is introduced. This approach saves energy of the nodes by avoiding the redundant rebroadcasting of the route request packets. The relaying status of the node is decided based on the broadcasting of its RREQ packets by its neighbors. And it helps in reducing routing overhead

incurred during the route discovery process. This energy efficient AODV protocol reduces energy consumption by 75-85% compared to AODV. A new mechanism called secure clustering and energy efficient protocol (SCEEP) is proposed in [5] to divide the MANET into a set of 2-hop clusters where each node belongs to at least one cluster. The nodes in each cluster elect a leader node (cluster head) to serve as the IDS for the entire cluster. To balance the resource consumption weight based leader election model is used, which elected an optimal collection of leaders to minimize the overall resource consumption and obtaining secure communication using Diffie-Hellman key exchange protocol. This model reduces the computation delay and is able to prolong the lifetime of MANET.

III. FUTURE RESEARCH DISCUSSION

Recent advances in mobile ad-hoc networks have led to many new protocols specifically designed for MANETs where energy efficiency and security are the essential considerations. Most of the attention, however, has been given to the routing protocols since they might differ depending on the application and network architecture. Power aware routing and secure routing are the main features of routing protocols used in the network. The resources present in MANET have limited battery power thus have limited life and are not easily rechargeable. So we have to reduce the energy consumption in MANET by using an efficient routing algorithm for data transmission. In mobile ad-hoc network, malicious nodes may attack the network to disrupt network activity thus security based algorithms are developed to avoid these types of attacks. The most commonly used routing protocol is ad-hoc on demand distance vector (AODV) routing protocol. A lot of changes have been carried out by the researchers in AODV protocol for increasing the security and efficiency of MANETs [7] [9] [10]. But there is not a single protocol which can give the best performance in ad-hoc network. Performance of the protocol varies according to the variation in the network parameters and ad-hoc network properties continuously vary. So, the choice of the protocol is the basis to perform in a particular type of network. Mobility of nodes changes the network topology is a prime concern. K arya et al. [10] presented two approaches to improve the performance of original AODV protocol. The proposed approach Secure-AODV increases the reliability of the routes between source and destination. The second approach Energy efficient-AODV decreases the energy consumption of the network. In this work an algorithm has been developed where dynamic change of routes are carried out when any chance of path breakage occurs by considering the node mobility and battery power simultaneously which helps in saving the network energy. Another objective here is to secure the network from the various types of packet dropping attacks. The proposed schemes can be incorporated into any Ad-hoc on demand routing protocol. This work can be further extended by designing trust based algorithm. . Simulation can be done in more scenarios with different node densities and higher mobility rates to evaluate the scalability and observe the performance of the network with higher speed of nodes.

IV. CONCLUSION

This paper presents a survey on various routing protocols in MANETs based on security and energy efficiency. The application of proposed algorithms produces better performance of the AODV protocol which is validated by simulation result. This work can be further extended by using DSR routing protocol to provide source routing and performance of this protocol can be compared with AODV. Simulation can be done in more scenarios with different node densities and higher mobility rates to evaluate the scalability and observe the performance of the

network with higher speed of nodes. However, on increasing the security and energy efficiency of the network, routing overhead increases due to which the cost of communication can also increases. Thus, for larger number of nodes routing overhead can also be taken into consideration with power saving and security to provide efficient communication.

REFERENCES

[1] J. Gomez, A. T. Campbell, M. Naghshineh, and C. Bisdikian, "Conserving transmission power in wireless ad hoc networks," in Proceedings of the 9th IEEE International Conference on Network Protocols., pp. 24–34, 2001.

[2] A. Mahimkar and R. K. Shyamasundar, "S-MECRA: a secure energyefficient routing protocol for wireless ad hoc networks," in Proceedings IEEE 60th Vehicular Technology Conference (VTC2004), vol. 4, pp. 2739–2743 Vol. 4, 2004.

[3] Floriano De Rango," Improving SAODV protocol with trust levels management, IDM and incentive cooperation in MANET", IEEE 2009.

[4] S.Preeti and B. Ramachandran, "Energy efficient routing protocols for mobile ad-hoc networks", IEEE 2011.

[5] Shobhana M and Suresh S, "Secure clustering andenergy based routing for mobile ad-hoc networks" in International journal of emerging technology and advanced engineering, volume 3, issue 3, march 2013.

[6] Ajay Jangra, Shivi Goel, "Biometric based Security Solutions for MANET: A Review", I. J. Computer Network and Information Security, 2013, 10, 44-50.

[7] Haidar Safa, Marcel Karam, and Bassam Moussa, "A Novel Power Aware Heterogeneous Routing Protocol for MANETs", in 2013 IEEE 27th International Conference on Advanced Information Networking and Applications.

[8] Ayesha Haider Ali, Faria Kanwal and Komal Bashir, "Centrally Coordinated Power Aware Route Selection for MANETs", in 2013 International Conference on Open Source Systems and Technologies (ICOSST).

[9] Golla Varaprasad, "High stable power aware multicast algorithm for mobile adhoc networks", in IEEE sensors journal, vol.13, no.5, may2013.

[10] K. V. Arya, Senior Member, IEEE, and Kuldeep Narayan Tripathi, "Power Aware and Secure Routing in Mobile and Ad-Hoc Networks", in 2013 IEEE 8th International Conference on Industrial and Information Systems, ICIIS 2013, Aug. 18-20, 2013, Sri Lanka.

[11] Arafat S.M. Qaed and T. Devi, "Secured Link Quality, Delay and Energy Aware Routing Protocol (SLQDEARP) For Mobile Ad Hoc Networks", in IEEE International Conference on Intelligent Interactive Systems and Assistive Technologies, August 2-3, 2013, Coimbatore, INDIA.