International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-2, December 2012

A Review of Energy Aware Routing Protocols in MANET

S.Nithya, S.K.Deepika, G.Sindhu

Abstract*— A Mobile Ad hoc Network (MANET) is a network consisting of a set of mobile hosts capable of communicating with each other without the assistance of base stations. This type of network having tiny light weighted nodes, with no clock synchronization mechanisms. In a MANET there are no dedicated routers and all network nodes must contribute to routing. Classification of routing protocols for MANET is based on how routing information is acquired and maintained by mobile nodes and/or on roles of network nodes in a routing. The wireless and distributed nature of MANETs poses a great challenge to system energy and the security.Mobile Ad hoc Networks (MANET) is a set of wireless mobile nodes dynamically form spontaneous network which works without centralized administration. Due to this characteristic, there are some challenges that protocol designers and network developers are faced with. These challenges include routing, service and frequently topology changes. Generally, in this type of network the exhaustion of energy will be more and as well, the security is missing due to its infrastructure less nature. There are also limited battery power and low bandwidth available in each node. Security attacks against MANET routing can be passive and or active. An overview of active attacks based on modification, impersonation/spoofing, fabrication, wormhole, and selfish behaviour is presented. A comparison of existing secure routing protocols form the main contribution in this paper, while some future research challenges in secure MANET routing are discussed

.

***Keywords*— Limited Battery Power, MANET, Routing Protocol, Routing Security**

I. INTRODUCTION

A traditional wireless network has an infrastructure with fixed base stations for mobile network hosts and/or mobile networks. Mobile devices coupled with wireless network interfaces will become an essential part of future computing environment consisting of infra-structured and infrastructure-less mobile networks. Wireless local area network based on IEEE 802.11 technology is the most prevalent infra-structured mobile network, where a mobile node communicates with a fixed base station, and thus a wireless link is limited to one hop between the node and the base station. The main contributions in this paper are: A classification of current relevant routing protocols for MANETs and their security ex-tensions, and a comparison of secure MANET routing protocols in regard to their protection and detection performance against several security attack types. (MANET) is an infrastructure-less multi hop network where each node communicates with other nodes directly or indirectly through intermediate nodes. Thus, all nodes in a MANET basically function as mobile routers participating in some routing protocol required for deciding and maintaining the routes. Since MANETs are self-organizing, rapidly deployable wireless networks, they are highly suitable for applications involving special outdoor events, communications in regions with no wireless infrastructure, emergencies and natural disasters, and military operations. Routing is one of the key issues in MANETs due to their highly dynamic and distributed nature. In particular, energy efficient routing may be the most important design criteria for MANETs since mobile nodes will be powered by batteries with limited capacity. Power failure of a mobile node not only affect the node itself but also its ability to forward packets on behalf of others and thus the overall network lifetime. The performance of a mobile ad hoc network mainly depends on the routing scheme.

Characteristics of MANET:

In MANET, each mobile host is autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

Multi-hop routing: Basic types of ad hoc routing algorithms can be single-hop and multi-hop. Single-hop MANET is simpler than multi-hop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other means for their energy. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions. Limited Security: MANETs are generally more prone to physical security threats than are fixed cable networks. The increased possibility of eavesdropping, spoofing and denial-of-service attacks should be carefully considered.

Our critical issue for almost all kinds of portable devices supported by battery power is power saving. Routing is one of the key issues in MANET due to its highly dynamic and distributed nature. Without power, any mobile device will become useless.

Manuscript published on 30 December 2012.
***** Correspondence Author (s)
S.Nithya, Asst.Professor, Dept Of ECE, KPR Institute of engineering and Technology, Coimbatore, India.
S.K.Deepika, Asst.Professor, Dept Of ECE, KPR Institute of engineering and Technology, Coimbatore, India.
G.Sindhu, Asst.Professor, Dept Of ECE, Kalaivani college of engineering and Technology, Coimbatore, India.

Battery power is a limited resource, and it is expected that battery technology is not likely to progress. Hence lengthen the lifetime of the batteries is an important issue, especially for MANET, which is all supported by batteries [1],[2],[3].

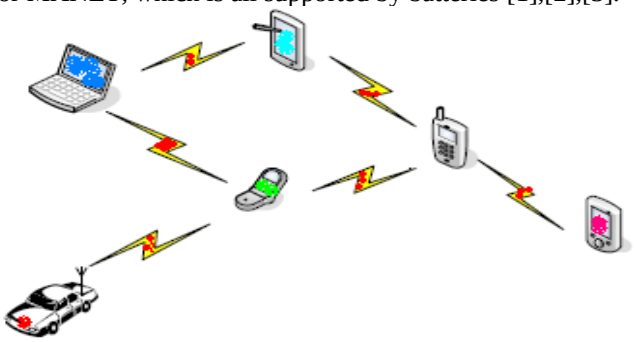
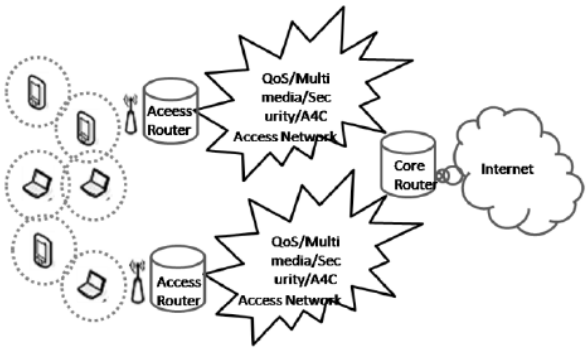


Fig 1: Ad Hoc Network Architecture

In a MANET every network host is also a base station for other network hosts and therefore network communications can be established on demand without the need for fixed network equipment. While MANETs bring many attractive features for future network communications they also introduce many challenges related to secure routing , energy efficient/power aware routing , scalability mobile agent based routing ,Quality of Service (QoS).



The main contributions in this paper are: A classification of current relevant routing protocols for MANETs and their security extensions, and a comparison of secure MANET routing protocols in regard to their protection and detection performance against several security attack types and to propose a new algorithm for the problem determined. And as well this paper showing how power aware routing must not only be based on node specific parameters (e.g. residual battery energy of the node), but must also consider the link specific parameters (e.g. channel characteristics of the link) as well, to increase the operational lifetime of the network. And also provides the security against route reply attacks using a check sum mechanism. It may also balance the traffic load in the network, while finding the reliable transmission path. Sleep/Active mode approach and Transmission Power Control Schemes are the main two methodologies, which are mainly responsible for considerable energy saving. The rest of the paper is organized as follows: In Section II, we provide an overview of the prior energy-aware routing algorithms in our own words. Then in Section III, we explain the energy aware secure routing algorithm. In Section IV, we present the simulation results, and we conclude our work in Section V

II. AN OVERVIEW OF RELATED WORK

2. Routing Protocols for MANET: Routing protocols for MANETs are usually classified into table driven/proactive protocols, on-demand/reactive protocols, and hybrid protocols based on how routing information is acquired and maintained by mobile nodes. Table driven/proactive protocols use a proactive routing scheme, in which every network node maintains consistent up-to-date routing information from each node to all other nodes in the network. On-demand/reactive protocols are based on a reactive routing scheme, in which at least one route is established only when needed. A hybrid routing protocol is a combination of proactive and reactive schemes with the aim of exploiting the advantages of both types of protocols.

Another classification into uniform and non-uniform routing protocols for MANETs is based on the network node roles in a routing scheme. In a uniform routing protocol all network nodes have the same role, importance and functionality. In a non-uniform routing protocol some network nodes carry out distinct management and/or routing functions. A uniform routing protocols is either reactive or proactive, while different classification schemes have been proposed for non-uniform routing protocol.

Table driven routing protocols have a low route acquisition delay because every node always has a fresh route to all other nodes in the network. However, the storage, bandwidth, and power requirements are high since each node must keep its routing table up-to date which mandates periodic routing message exchanges. On-demand protocols incur a much lower load on the network, compared to table driven, since each node does not need to constantly keep their routing tables up-to-date. However, route acquisition delay is high since routing messages must be exchanged every time before communication is possible over a new route, based on reactive routing schemes.

Ad hoc On-demand Distance Vector (AODV)

In AODV, when a node wants to communicate with another, the source node floods the network with route request (RREQ) messages. If a node that receives a RREQ packet is not the destination or doesn't have a fresh route to the destination it creates a reverse route to the source (a route back to source with the node from where the RREQ came from as next hop). If the receiver of a RREQ is the destination node, it sends a route reply (RREP) message back to the source as a unicast packet over the route it received the RREQ. The destination node only sends a RREP to the first RREQ message it receives. Every node receiving a RREP also creates a route to the destination in the routing table. As a result, when the RREP reaches the source, all nodes in the shortest route path will have a route both to the source and destination.

Dynamic Source Routing (DSR)

As with AODV, DSR floods the network with route request messages as a result of route discovery initiation. However, compared with AODV, the destination node returns a route reply for each copy of route request message it receives. As a result, the source node will know more than one route to the destination node upon reception of all route replies. The addresses of all nodes through which both route request and route reply messages have traversed are added to the routing message headers, so a node knows not only the hop count values of all routes to a destination, but also all the intermediate nodes.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Based on hop count and other route information, the source node finally selects the route with the lowest latency. Each data packet carries, in its header, the complete ordered list of intermediate nodes through which a packet is to be transmitted. DSR has lower network overheads compared with AODV, mainly due to the multiple storage and source routing features. If a link fails, the source node does not need to re-initiate route discovery, as in AODV. Instead it selects another route from its routing table. Since the route information is included in all data packets, other nodes forwarding or overhearing any data packet can cache the routing information for future use, which also eliminates the need for route discovery if the route is still fresh.

Hybrid Protocol: proactive scheme is used to discover routes to nearby nodes and reactive schemes are used to discover long distance nodes. An example of a hybrid routing protocol is Zone Routing Protocol .ZRP is also called a hierarchical routing protocol where the network can be grouped in clusters, trees, or zones where one node is chosen to be a leader that manages that particular routing area.

Hybrid protocols provide a lower route acquisition delay than reactive protocols and a lower overhead than proactive protocols. These protocols, however, are not suitable for highly dynamic MANET environments since in such network conditions it is simply infeasible to delegate roles to nodes and divide the network into zones.

2.1 Existing Energy aware Routing Schemes:

Mobile ad hoc network (MANET) is an infrastructure-less multi hop network where each node communicates with other nodes directly or indirectly through intermediate nodes. Thus, all nodes in a MANET basically function as mobile routers participating in some routing protocol required for deciding and maintaining the routes. Among the various network architectures, design of the mobile ad hoc networks (MANET) plays an important role. Such a network can either operate in a standalone fashion with the ability of self-configuration and no clock synchronization mechanism. Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks where, the structure of the network changes dynamically. No base stations are supported in such an environment, and mobile hosts may have to communicate with each other in a multi-hop fashion. Minimal configuration and fast deployment make MANETs suitable for emergency situations like natural or human-induced disasters and military conflicts. Mobile devices coupled with wireless network interfaces will become an essential part of future computing environment consisting of infra-structured and infrastructure-less mobile networks.

Energy management in wireless networks is very important due to the limited energy availability in the wireless devices. It is important to minimize the energy costs for communication as much as possible by practicing energy aware routing strategies. Based on the observations of signal attenuations, many routing protocols are operated. Energy aware routing algorithm would select a route comprising multiple short distance hops over another one with a smaller hop count but larger hop distances. The PAMAS (Power aware Multi access protocol with signaling) [6] protocol allows a host to power its radio off when it has no packet to transmit/receive or any of its neighbors is receiving packets, but a separate signaling channel to query neighboring hosts' states is needed. In PAMAS, [7] they provide several sleep patterns and it allows the mobile nodes to select their sleep patterns based on their battery power. But this needs a special hardware called RAS (Remote Activated Switch). But they biased towards smaller hops typically led to the selection of paths with a very large hop count.

The PARO [7], [8] has proposed for the situation where the networks having the variable transmission energy. This protocol essentially allows an intermediate node to insert itself in the routing path if it detects potential savings in the transmission energy. Later, Connected-dominated set based power saving protocol is proposed. In which some hosts must as a coordinators, which are chosen according to their remaining battery energies and the numbers of neighbors they can connect .In this type of network, only coordinators need to awake, other hosts can enter the sleeping mode.

Min-Hop routing is the conventional "energy unaware" routing algorithm, where each link is assigned based on the identical cost. In which it simply selects the routes based upon the number of hops. Less number of hop counts path is considered as a route for transmission of packets. Thus results in less reliability and power wastage. Min Energy routing is another power aware routing algorithm, which simply selects the path corresponding to the minimum packet transmission energy for reliable communication, without considering the battery power of individual nodes. In which the number of hops and delay increases. This results in less energy consumption but with less reliability

The MTPR mechanism uses a simple energy metric, represented by the total energy consumed to forward the information along the route. This way, MTPR reduces the overall transmission power consumed per packet, but it does not affect directly the lifetime of each node (because it does not take account of the available energy of network nodes). Notice that, in a fixed transmission power context, this metric corresponds to a Shortest Path routing. Huaizhi Li and Mukesh Singhal [9] have presented an on-demand secure routing protocol for ad hoc networks based on a distributed authentication mechanism. The protocol has made use of recommendation and trust evaluation to establish a trust relationship between network entities and it uses feedback to adjust it. The protocol does not need the support of a trusted third party and it discovers multiple routes between two nodes. Sec AODV [10] is the one of the protocol that incorporates security features of non-repudiation and authentication, without relying on the availability of a Certificate Authority (CA) or a Key Distribution Center (KDC).

They have presented the design and implementation details of their system, the practical considerations involved, and how these mechanisms are used to detect and thwart malicious attacks.

Packet conservation Monitoring Algorithm (PCMA) [11] can be used to detect selfish nodes in MANETs. Though the protocol addresses the issue of packet forwarding attacks, it does not address other threats.

Syed Rehan Afzal et al. [12] have explore the security problems and attacks in existing routing protocols and then they have presented the design and analysis of a secure on-demand routing protocol, called RSRP which has confiscated the problems mentioned in the existing protocols.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Moreover, unlike Ariadine, RSRP has used a very efficient broadcast authentication mechanism which does not require any clock synchronization and facilitates instant authentication.

Secure Routing Protocols for MANET:

Secure routing protocols for MANETs are usually derived as extensions of existing routing protocols, the main features of trust within a MANET are defined as,

A decision method to determine trust against an entity should be fully distributed since the existence of a trusted third party (such as a trusted centralized certification authority) cannot be assumed, Trust should be determined in a highly customizable manner without excessive

Computation and communication load, while also capturing the complexities of the trust relation-ship. A trust decision framework for MANETs should not assume that all nodes are cooperative. In resource-restricted environments, selfishness is likely to be prevalent over cooperation, for example, in order to save battery life or computational power, Trust is dynamic, not static, Trust is subjective, Trust is not necessarily transitive. The fact that A trusts B and B trusts C does not imply that A trusts C. Trust is asymmetric and not necessarily reciprocal. Trust is context-dependent. A may trust B as a wine expert but not as a car fixer. Similarly, in MANETs, if a given task requires high computational power, a node with high computational power is regarded as trusted while a node that has low computational power but is not malicious (i.e., honest) is distrusted.

Ariadne

Ariadne is a secure reactive (on-demand) routing protocol based on DSR that provides authentication of routing messages. Authentication can be performed by using shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signatures. Ariadne is based on the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol which is broadcast authentication procedure requiring relaxed time synchronization. It consists of two steps: authentication of routing messages, verification that there is no node missing in the routing message headers.

Security aware ad hoc routing:

The SAR protocol incorporates security attributes as parameters into ad hoc route discovery. It enables the use of security as a negotiable metric with the intention to improve the relevance of the discovered routes. While AODV discovers the shortest path between two nodes, SAR can discover a path with desired security attributes. For instance, the criteria for a valid route can be that every node in the route must own a particular shared key. In such a case, routing messages would be encrypted with the source node's shared key and only the nodes with the correct key can read the header and forward that routing message. As a result, if a routing message reaches the destination, it must have been travelled through nodes having the same trust level as the source node. It is then for the node initiating the route discovery to decide upon the desired security level for that route. SAR has been presented as an extension to AODV but it can also be extended to any existing routing protocol. Due to strong cryptographic protection of routing messages, attacks such as modification, impersonation, and fabrication are effectively eliminated. A major problem with SAR, however, is that it involves significant encryption overhead since each intermediate node has to perform both encryption and decryption operations.

Secure efficient ad hoc networks (SEAD)

SEAD is a proactive routing protocol based on DSDV. SEAD uses a hash chain method for checking the authenticity of data packets and the hash chain value is used for transmitting routing updates. The authentication of each entry of a routing update message is verified by a receiving node. Looping is removed by using a sequence number and authentication of the source of routing update message. Authentication of the source can be done for example by providing a shared secret key between each pair of nodes in the MANET which is then used for MAC calculations between the nodes for the authentication of a routing update message.

SEAD provides strong protection against attackers trying to create incorrect routing state in other nodes by for example modifying the sequence number in the routing packet. However, SEAD does not protect against an attacker tampering the next hop or the destination field of a routing update packet.

Syed Rehan Afzal et al. [12] have explore the security problems and attacks in existing routing protocols and then they have presented the design and analysis of a secure on-demand routing protocol, called RSRP which has confiscated the problems mentioned in the existing protocols. Moreover, unlike Ariadne, RSRP has used a very efficient broadcast authentication mechanism which does not require any clock synchronization and facilitates instant authentication.

III. PROPOSED SYSTEM

A mobile node consumes its battery energy not only when it actively sends or receives packets but also when it stays idle listening to the wireless medium for any possible communication requests from other nodes. Thus, energy efficient routing protocols minimize either the active communication energy required to transmit and receive data packets or the energy during inactive periods. Secondly, Security is a more sensitive issue in MANETs than any other networks due to lack of infrastructure and the broadcast nature of the network. While MANETs can be quickly set up as needed, they also need secure routing protocols to add the security feature to normal routing protocols. The need for more effective security measures arises as many passive and active security attacks can be launched from the outside by malicious hosts or from the inside by compromised nodes. Key management is a fundamental part of secure routing protocols; existence of an effective key management

framework is also paramount for secure routing protocols. Several security protocols have been proposed for MANETs, there is no approach fitting all networks, because the nodes can vary between any devices. Our newly proposed secure energy efficient algorithm holds two mechanisms.

Energy is a scarce resource in ad hoc wireless networks and it is of paramount importance to use it efficiently when establishing communication patterns.

Energy Management is defined as the process of managing the sources and consumers of energy in a node or in a network as a whole for enhancing the lifetime of the network.

Transmission Power Management: The power consumed by the radio frequency (RF) module of a mobile node is determined by several factors such as the state of operation. The transmission power, and the technology used for the RF circuitry. The state of operation refers to transmit, receive, and sleep modes of operation. The transmission power is determined by the reachability requirement of the network, the routing protocol and the MAC protocol employed. The RF hardware design must ensure minimum power consumption in all the three stages of operation.

Battery Energy Management: The battery management is aimed at extending the battery life of a node by taking advantage of its chemical properties, discharge patterns, and by the selection of a battery from a set of batteries that is available for redundancy.

3.1. Energy efficient mechanism:

This mechanism deals with the reduction of energy consumption. It makes all the active state nodes to sleep when not in use by means of active sleep state methodology. This Active /sleep state methodology initially categorize the energy as active communication energy and inactive communication energy. The active communication energy was reduced by adjusting the power of the each node to reach only the particular destination and not more than that. The inactive communication energy was reduced by simply turns off the node during the idle case. This leads to considerable energy savings, especially when the network environment is characterized with low duty cycle of communication activities. Secondly, it will find the route with least cost path based on the reliability and the residual battery energy. This algorithm assumes RREQ (Repeat Request) for reliable packet transmission in each hop. If the packet or its acknowledgement is lost, the sender will retransmit the packet. To formulate this algorithm, assume E be the energy expected by the node to transmit the packets from source to destination.

E (i, j) -> Expected Energy to Transmit a Packet
B (i) -> Total Residual Battery Energy
R= B-E-> Remaining Residual Battery Energy

The ratio of the fraction of residual battery energy to be consumed to the total residual battery energy (B) gives the link weight. The path with less weight is to be selected. The Link weight is defined as the fraction of the residual battery energy that node i consumes to transmit a packet reliably over (i, j). Link weight is determined using Dijkstra's algorithm.

Link Weight= E (i, j)/B (i)

If the residual energy of the nodes is not considered, then the energy in the best path's node will be consumed more than the other nodes in the network. In this model the consumed energy by a node during packet transmission consists of two elements. The first element is the energy consumed by the processing part of the transceiver circuit, and the second element is the energy consumed by the transmitter amplifier to generate the required power for signal transmission.

3.2 Energy Management Scheme

In Ad-hoc network, the packets are transmitted with minimum power, which is required for decoding the packets. In such a situation, TPC (Transmission Power Control) scheme is used. This transmission power control approach can be extended to determine the optimal routing path that minimizes the total transmission energy required to deliver data packets to the destination. In wireless communication transmission power has strong impact on bit error rate, and the inter radio interference. Thus this transmission power control scheme which will adjust the transmission power of the node based on the link distance. If TPC is not present, then the maximum transmission power is utilized. If the residual energy of the nodes is not considered, then the energy in the best path's node will be used more unfairly than the other nodes in the network. Because of their battery depletion, these nodes may fail after a short time, whereas other nodes in the network may still have high energy in their batteries.

3.3 Security Scheme:

This mechanism deals with the security aspects. In order to make our proposed algorithm more secure, a new cryptographic check sum mechanism is used. The proposed algorithm is very effective as it detects the malicious node quickly and it provides security against the attacks. Among all the security services, authentication is probably the most complex and important issue in MANETs. Cryptographic mechanisms make use of a hash code. Hash code does not use a key but is a function only of the input message. The message plus concatenated hash code is encrypted using symmetric encryption. In this proposed algorithm, initially once a node S want to send a packet to a destination node D, it initiates the route discovery process by constructing a route request RREQ packet. It contains the source and destination ids and a request id. When an intermediate node receives the RREQ packet for the first time, it appends its id to the list of node ids and signs it with a key which is shared with the destination. It then forwards the RREQ to its neighbors.

When the destination receives the accumulated RREQ message, it first verifies the sender's request id by re computing the sender's MAC value, with its shared key. It then verifies the digital signature of each intermediate node. If all these verifications are successful, then the destination generates a route reply message RREP.

If the verifications fail, then the RREQ is discarded by the destination. It again constructs a MAC on the request id with the key shared by the sender and the destination.

Secondly, the message and the hash function are concatenated. Then the concatenated hash code along with the message is encrypted using symmetric key encryption. The bank block indicates the encrypted value of concatenated hash code with message. The Message must be transferred only between the source and the destination using the secret key, thus the data transmission is more secure and has not been altered. The comparative block predicts the absolute key value with secured message. The hash code provides the structure or redundancy required to achieve authentication. Because encryption is applied to the entire message plus hash code, Confidentiality is also provided. If in the case of many intermediate states present between the source and the destination, then the security is achieved by means of digital signatures. Thus, our new secure energy efficient algorithm with these two mechanisms enhances the routing problem and manages the network resources of achieving fair resources usage across the network node with higher security.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

IV. PERFORMANCE EVALUATION

4.1 Simulation model:

Consider an ad hoc network in which nodes are uniformly distributed in a square area. In the network, sessions are generated between randomly chosen source-destination nodes with exponentially distributed inter-arrival time. The source node of the session transmits data packets with the constant rate 1 packet/sec. We developed our simulation model using ns 2.34 simulator. The ns 2.34 simulator allows extracting from a simulation many interesting parameters, like throughput, data packet delivery ratio, end-to-end delay and overhead, [16]. To have detailed energy-related information over a simulation, we modified the ns 2.34 simulator code to obtain the amount of energy consumed over time by type (energy spent in transmitting, receiving, overhearing or in idle state), [17]. This way, we obtained accurate information about energy at every simulation time. We used these data to evaluate the protocols from the energetic point of view: we will see the impact of each protocol on different new parameters, like the number of nodes alive over time (to check the lifetime of nodes), the expiration time of connections (to see the network lifetime), and the energy usage divided by type (receiving, transmitting, overhearing).

4.1.1 Practical Considerations:

The routing protocols for MANET'S are generally categorized as table driven, and on demand driven based on the timing of when the routes are updated. SEER algorithm can be implemented with the existing routing protocols for ad hoc networks. Here, we implemented with AODV as the routing protocol. The algorithm performance was compared with the normal AODV protocol. An AODV is an on demand routing protocol that combines the capabilities of both DSR and DSDV protocol. It uses route discovery and route maintenance from DSR and in addition to the hop by hop routing sequence numbers and periodic beacons from Destination-Sequenced Distance vector (DSDV) routing protocol. AODV is an on demand routing protocol in which routes are discovered only when a source node desires them. Route discovery and route maintenance are two main procedures: The route discovery process involves sending route-request packets from a source to its neighbor nodes, which then forward the request to their neighbors, and so on. Once the route-request reaches the destination node, it responds by uni casting a route-reply packet back to the source node via the neighbor from which it first received the route request. When the route-request reaches an intermediate node that has a sufficiently up-to-date route, it stops forwarding and sends a route-reply message back to the source. Once the route is established, some form of route maintenance process maintains it in each node's internal data structure called a route-cache until the destination becomes inaccessible along the route. Note that each node learns the routing paths as time passes not only as a source or an intermediate node but also as an overhearing neighbor node.

Table1: Simulation

Area Size	1000 X 1000
Simulation time	400 s
Number of Nodes	11
MAC type	MAC 802.11
Traffic Source	CBR
Initial Energy	1000 J
Packet Size	512 Bytes
Routing Protocol	AODV
Nodes Speed	3 m/s
Beacon Period	200 ms

4.1.2 Simulation Results

The following results show the operation of new secure energy aware algorithm. Some parameters like packets received, Energy consumption per packet transmission, end to end latency and packet delivery ratio Throughput are analyzed to verify the performance of the new power aware mechanisms. As dealing with the energy and security aspect, our model AODV protocol was compared with other existing protocols such as RSVP and SAODV Protocol. Our New model AODV (Secure Energy aware Mechanism) shows good energy efficiency when compared with the all other existing protocols.

Energy Consumption per packet:

It defines the energy consumed by a node to transmit a packet from source to destination. In the below graph we compared the plain AODV protocol with our new secure energy aware mechanism. By means of new secure energy aware mechanism the power consumed by the node to transmit to the packet was decreased at a higher rate. The energy consumption per packet was decreased as previous. This will highly increases the network life time.

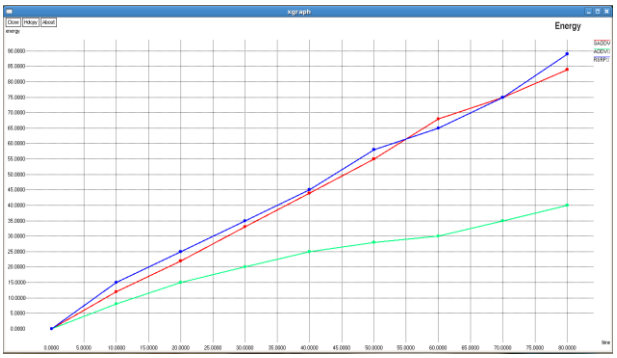


Fig 3: Energy Consumption per Packet

Packet delivery ratio:

Data packet delivery ratio can be calculated as the ratio between the number of data packets that are sent by the source and the number of data packets that are received by the sink. This is the amount of successful received bits at the destination nodes for the entire simulation period. Packet delivery ratio should be always high for the efficient algorithm or a protocol. The figure 4 shows the packet delivery ratio was high when compared with the previous methodology.

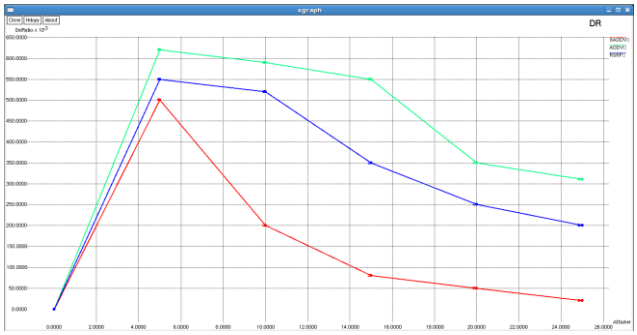


Fig 4: Packet delivery ratio

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

End To End Latency:

End-to-end Latency refers to the time taken for a packet to be transmitted across a network from source to destination.End to end latency which includes all possible delays caused by buffering during route discovery time, queuing at the interface queue, retransmission, and processing time. It defines the ratio of interval between the first and the second packets to a total packets delivery. This figure 5 shows the result of end to end latency.

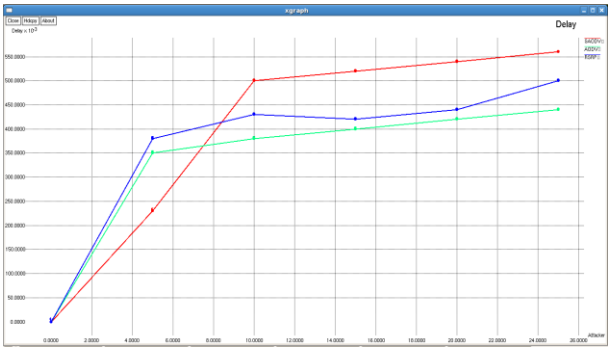


Fig 5: End To End Latency

The end to end latency of the new secure energy aware mechanism was highly reduced when compared with normal protocol operations.

V. CONCLUSION

In this paper, a new secure energy aware routing algorithm was proposed. It mainly defines the least cost path based on the reliability and the remaining energy of the node for packet transmission from, source to destination, and making the sleep/active state methodology for providing the energy efficiency. Later this algorithm provides a new cryptographic check sum mechanism to prevent the communications from attackers. By means of these features, we may effectively secure our data's with minimal energy consumption Thus; this algorithm can effectively reduce the energy consumed by the node as well as increases the security and reliability of the network. This in turn increases the operational lifetime and it maintains the load traffic as well.

REFERENCES

[1]. X.-Y. Li, Y. Wang, H. Chen, X. Chu, Y. Wu, and Y. Qi, "Reliable and energy-efficient routing for static wireless ad hoc networks with unreliable links," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 10, pp. 1408–1421, 2009.

[2]. B. Mohanoor, S. Radhakrishnan, and V. Sarangan, "Online energy aware routing in wireless networks," Ad Hoc Networks, vol. 7, no. 5, pp. 918–931, July 2009.

[3]. Ashwani kush ,Divya Sharma, Sunil Taneja, "A Secure and Power Efficient Routing Scheme for Ad Hoc Networks", International journal of Computer Applications, Volume 21-No 6, May 2011

[4]. V. Kanakaris*, D. Ndzi and D. Azzi., Ad-hoc Networks Energy Consumption: A review of the Adhoc Routing Protocols, Journal of Engineering Science and Technology Review 3 (1) (July 2010).

[5]. Dr. A. Rajaram, J. Sugesh, Power Aware Routing for MANET using on Demand Multi path Routing Protocol, International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011.

[6]. Dhiraj Nitnaware1 & Ajay Verma, "Performance Evaluation of Energy Consumption of Reactive Protocols under Self-Similar Traffic", International Journal of computer science and communication vol.1, No.1, January-June 2010.

[7] Busola S.Olagbegi and Natarajan Meganathan "A Review Of the Energy Efficient and Secure Multicast routing protocols for mobile ad hoc networks", International journal on applications of graph theory in wireless ad hoc networks and sensor networks,Vol 2, No.2, June 2010

[8]. J. Gomez, A. T. Campbell, M. Naghshineh, and C. Bisdikian, "Paro: supporting dynamic power controlled routing in wireless ad hoc networks," Wireless Networks, vol. 9, no. 5, pp. 443–460, 2003.

[9]. Huaizhi Li and Mukesh Singhal, 2006."A Secure Routing Protocol for Wireless Ad Hoc Networks", in proceedings of 39th Annual Hawaii International Conference on System Sciences, Vol.9.

[10]. A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis and Y. Yesha, 2008. "Thresholdbased intrusion detection in ad hoc networks and secure AODV", Vol.6, No.4, pp.578-599.

[11]. Tarag Fahad & Robert Askwith, 2006. "A NodebMisbehaviour Detection Mechanism forbMobile Ad-hoc Networks" The 7th Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting.

[12]. M. Mohammed, Energy Efficient Location Aided Routing Protocol for Wireless MANETs, International Journal of Computer Science and Information Security, vol. 4, no. 1 & 2, 2009.

[13]. J. Vazifehdan, R. Hekmat, R. V. Prasad, and I. Niemegeers, "Performance evaluation of power-aware routing algorithms in personal networks," in The 28th IEEE International Performance Computing and Communications Conference (IPCCC '09), pp. 95–102, Dec. 2009.

[14]. Wang Yu, "Study on Energy Conservation in MANET", Journal of Networks, Vol. 5, No. 6,June 2010.

[15]. Niranjan Kumar Ray & Ashok Kumar Turuk, (2010) "Energy Efficient Techniques for Wireless Ad Hoc Network", International Joint Conference on Information and Communication Technology,pp105-111.

[16]. Ns-2 network simulator, http://www.isi.edu/nsnam/ns/, 1998.

Nithya.S is with the ECE department in KPR Institute of Engineering &Technology, Coimbatore as Assistant professor. She has done her ME Communication systems in Sri Shakthi Institute of Engineering & Technology, Coimbatore. She has done her BE in ECE from Sengunthar Engineering college, Tiruchengode, Tamil Nadu. Her research interests include mobile adhoc networks. She has presented papers in international and national conferences. She has also published papers in international journals.

Deepika.S.K is with the ECE department in KPR Institute of Engineering &Technology, Coimbatore as Assistant professor. She has done her ME Communication systems in Sri Shakthi Institute of Engineering & Technology, Coimbatore. She has done her BE in ECE from Anna university,Coimbatore, Tamil Nadu.Her research interests include Sensor networks. She has presented papers in international conference and Journals

Sindhu.G is with the ECE department in kalaivani college of Engineering &Technology, Coimbatore as Assistant professor. She has done her ME Communication systems in Sri Shakthi Institute of Engineering & Technology, Coimbatore. Her research interests include mobile adhoc networks. She has presented 2 papers in international conference