Improved Key Management And Security in Dynamic Wireless Sensor Networks

Anitha.M[1], Gomathi.P.M[2]
[1, 2] Department Of Computer Science
[1, 2] P.K.R Arts college for Woman, Gobichettipalayam

Abstract- *Recently, wireless sensor networks (WSNs) have been deployed for a wide variety of applications, including military sensing and tracking, patient status monitoring, traffic flow monitoring, where sensory devices often move towards different locations. Securing the data and communications requires suitable encryption route key protocols certificate less-effective encrypted route key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The CL-EKM supports efficient route key updates when a node leaves or joins a cluster and ensures forward and backward route key secrecy. protocol also supports efficient route key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links. A security analysis of our scheme shows that protocol is effective in defending against various attacks. CL-EKM in Ubuntu OS and simulate it using Network simulator to assess its time, energy, communication, and memory performance.*

As wireless sensor networks are growing, the need for effective security mechanisms is doing so. In this paper, propose Energy-Efficient Route key Management system Protocol, a cryptographic route key management protocol, which is based on the location based group route key scheme. The protocol supports the revocation of the compromised nodes and the energy-efficient reroute keying. The design of the protocol is motivated by the observation that a unicast-based reroute keying is not suitable for meeting the security requirements of periodic reroute keying in wireless sensor networks. Our protocol supports the broadcasting - based reroute keying for low-energy route key management and high resilience. For increasing complexity of encryption route key, we use dynamic composition route key scheme. Our protocol provides group management protocols for secure group communication.

Keywords- VANETS, Multi path routing, Ad-hoc On-Demand Multipath Distance Vector Routing, Hybrid Multi-rate Multipath Routing

I. INTRODUCTION

Human A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on [2]. These sensor nodes can communicate over short distance via a wireless medium and cooperate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control. In many WSN applications, the deployment of sensor nodes is performed in an ad hoc fashion without careful planning. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding [4].

Mobile networking is one of the most important technologies which support pervasive computing. During the last decade, advances in both hardware and software techniques have resulted in mobile and wireless networking. Vehicular ad hoc networks(VANETS) are wireless networks without any fixed infrastructure. These are usually set up on a temporary basis to serve a particular purpose within a specific period of time [1]. A mobile ad-hoc network (VANET) is a multi-hop wireless network formed by a group of mobile nodes that have wireless capabilities and are in closeness of each other. VANET facilitate communication among mobile users in military or civil emergency where fixed infrastructure is infeasible. Most VANETS are based on IEEE 802.11 or Wi-Fi medium access control (MAC) standard due to external noise and interference from transmissions and mobility, the routes in a VANET break frequently. The Dynamic Source Routing (DSR) is one of the widely used routing protocols for VANET [3]. Because of security is considered to improve its performance when compared to other protocols. This paper describes a comparison of various protocols which are used in VANET to overcome several issues faced by network transmission.

The rest of this paper is organized as follows. Section II provides the brief review of routing protocol in VANETS. Section III provides the details various methodology of routing protocols. Section IV shows the Experimental results to evaluate the performance and comparison Section V includes conclusion

II. RELATED WORKS

Numerous schemes have been proposed for secure routing protocols, and Intrusion Detection and Response Systems, for ad hoc networksAnandPatwardhanet.al (2005) proposed for secure routing protocols, and Intrusion Detection and Response Systems, for ad hoc networks. A concept implementation of a secure routing protocol based on AODV over IPv6, are further reinforced by a routing protocol-independent Intrusion Detection [4] and response system for ad-hoc networks Security features in the routing protocol which include mechanisms for non-repudiation, authentication using Statistically Unique and Cryptographically Verifiable (SUCV) identifiers, without relying on the availability of a Certificate Authority (CA), or a Route route key Distribution Center (KDC). Yih-Chun Hu et.al (2003)evaluated the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol [2] . In order to support the use of nodes with limited CPU processing capability, and to guard against Denial of-Service (DoS) attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, by use of efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol.

Nadkarniet.al (2003) proposed misuse detection - based IDS for VANETSs. The protocol-independent design makes use of a self-adjusting threshold scheme and detects a priori known attack patterns with over 90% accuracy and is generally insensitive to false alarms [3]. Lu et.al (2009) proposed a AODV suffering black hole attack BAODV (Bad Ad Hoc On-demand Distance Vector Routing suffering black hole attack) which can simulate black hole attack to VANETS by one of nodes as a malicious one in network [1]. BAODV can be regarded as AODV, which is used in VANETS exited black hole attack. The SAODV protocol is used to address the security weakness of the AODV protocol and is capable of withstanding the black hole attack.

Johnsonet.al (2007) presents a protocol for routing in ad hoc networks that uses dynamic source routing. The protocol adapts quickly to routing changes when host movement is frequent, yet it requires little or no overhead during periods in which hosts move less frequently [5]. The difference in length between the routes used and the optimal route lengths is negligible, and in most cases, route lengths are on average within a factor of 1.01 of optimal. Campet.al (2002) presents a survey of mobility models that are used in the simulations of ad hoc networks [7]. It describe several mobility models that represent mobile nodes whose movements are independent of each other and several mobility models that represent mobile nodes whose movements are dependent on each other The goal of this paper is to present a number of mobility models in order to offer researchers more informed choices when they are deciding upon a mobility model to use in their performance evaluations.

III. METHODOLOGY

A. Destination-Sequenced Distance Vector (DSDV)

Destination sequenced distance vector routing (DSDV) is modified from the Routing Information Protocol (RIP) to ad hoc networks routing. DSDV adds a new feature and sequence number, to each route table entry. By using the newly added sequence number, then the mobile nodes can distinguish old route information from the new table and it can prevent the formation of routing loops. In DSDV, each mobile node of an ad hoc network which maintains a routing table, which listed all available destinations, the metric and next hop to each destination and a sequence number are generated by the destination node. The routing table stored in each mobile node, and then the packets are transmitted between the nodes of network. Each node of the ad hoc network updates the routing table periodically or with new information available to maintain the consistency of the routing table with the changing topology of the network [13]. The main purpose of DSDV is to address the looping problem of the distance vector routing protocol and to make the distance vector routing more suitable for ad hoc networks routing. However, DSDV causes a route fluctuation because of its route updates. At the same time, DSDV does not solve the common problem of all distance vector routing protocols and the unidirectional links problem

B. Ad hoc On-demand Distance Vector (AODV)

AODV supports dynamic, self-starting, multi-hop routing between mobile nodes and maintain an ad hoc network. AODV enables for the construction of routes to specific destinations and it does not require that nodes when they are not in active communication. AODV avoids the counting to infinity‖ problem by using destination sequence numbers. This makes AODV loop free. AODV can be defined by 3 message types such are Route Requests (RREQs) messages are used to initiate the route finding process, Route Replies (RREPs) messages are used to finalize the routes and Route Errors (RERRs) messages are used to notify the network of a link breakage in a route. The Path Discovery process is initiated whenever a source node needs to communicate with another node for which it has no routing information in its table list. Every node should maintain two separate counters which are a node sequence number and a broadcast id. If the source node initiates path discovery by broadcasting a route request (RREQ) packet to its neighbors then it keeps track of the following information to implement the reverse path setup as well as the forward path is shown in Fig 1 and Fig 2 setup that will accompany the transmission protocol (RREP). There are two sequence numbers which are included in a RREQ such as the source sequence number and the last destination sequence number known (source) [12]. The source sequence number is used to maintain freshness information about the reverse route to the source and the destination sequence number which specifies how fresh a route to the destination must be before when it can be accepted by the source.

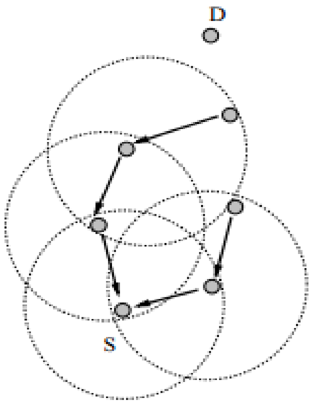

Figure 1. Reverse Path Formation

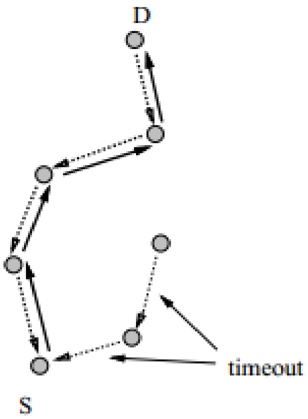

Figure 2. Forward Path Formation

The main difference between DSR and AODV is that the way they keep the information about the routes while in DSR it is stored in the source but while in AODV it is stored in the intermediate nodes. However, the route discovery phase of both is based on flooding. This means that all nodes in the network should participate in every discovery process, regardless of their potential in actually contributing to set up the route or not, thus increasing the network load.

C. Dynamic Source Routing

One of the most widely referred routing algorithms in VANETS is the DSR protocol. Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. The Dynamic Source Routing protocol (DSR) is a very simple and efficient routing protocol which is designed in such away specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to beself-organizing (It determines how best to move packets around) and self-configuring (It determines the routes available) without the need for any existing network infrastructure. Each node in the network which maintains a route cache [5]. To send data to another node, if a route is found in its route cache, the sender puts this route (a list of all intermediate nodes) in the packet header and it transmits to the next path. Each intermediate node examines the header and retransmits it to the node. If no route is found, the sender buffers the packet and obtains a route.

DSR has two basic modes of operation, which are route discovery and route maintenance

a) Route Discovery

Route discovery includes route request RREQ and route reply RREP messages. In route discovery phase, if a node wishes to send a message, at first it broadcasts an RREQ packet to its neighbors. Every node within the broadcast range adds their node ID to the RREQ packet and rebroadcasts. The broadcast messages will reach through route on the destination or a same node. Since each node maintains a route cache, which is a buffer for routes by a node, it first checks its cache for a route which matches the requested destination before rebroadcasting the RREQ packet. By maintaining a route cache in every node it reduces the overhead generated by a route discovery phase. If a route is found in the route cache, then the node will return an RREP message to the source node rather than forwarding the RREQ message further in the network. For example Figure 3 shows a diagrammatic representation of the route discovery phase. In the figure it consists of four nodes; A, B, C and D where nodes A and D are the source and destination nodes respectively. When A wants to send data packets (DP), it first checks its route cache whether it has a direct route to D [8]. If it does not have a route then it find a route to D by broadcasts an RREQ message to its neighbours. When B receives the RREQ message, it stores the route AB and also it checks whether it has a route to D in its route cache. If it finds a route to D, it sends an RREP message to A which in turn initiates the sending of the data packet to D via the discovered route. If B does not find a route to D in its cache, it rebroadcasts the RREQ message to its neighbours. The process continues until the RREQ message reaches D, assuming that there is no intermediate node has a route to D. When D gets the RREQ message it stores routes AB, BC, and CD in its cache and forwards an RREP message to A which on reception of the message commences the sending of data packet through the discovered route.

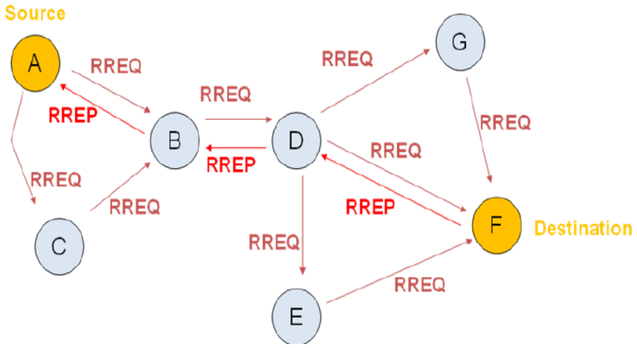

Figure 3. Route Discovery Mechanism

b) Route Maintenance Phase

In route maintenance phase there are two types of packets are used namely; route error (RERR), and acknowledgements (ACK). DSR ensures the validity of the existing routes which is based on the ACK received from the neighboring nodes then the data packets have been transmitted to the next hop successfully. Acknowledgement packets include passive acknowledgements as the node which overhears the next neighbor forwarding the packet which en route to the destination. An RERR packet is generated when a node encounters an obstacle in transmission, implying that a node has failed to receive an ACK message. This RERR packet is sent to the source node in order to re-initiate a new route discovery phase if an alternative route to the destination cannot be found. After receiving the RERR message, nodes remove the route entries that use the broken link from their route caches. An example route maintenance mechanism is shown in Figure 4. In the figure, when C does not receive an ACK message from the destination node D then it senses an obstacle along route CD and sends an RERR message to the source node A, which seeking for an alternative route to forward data packets to D, rather on a fresh route discovery process.

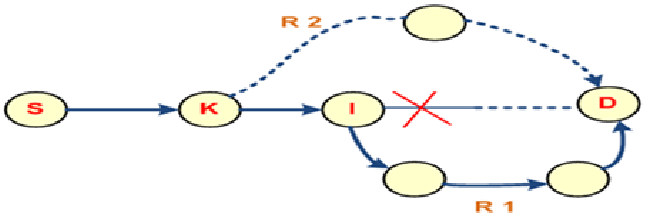

Figure 4. Route Discovery Mechanism

Conventional DSR does not possess most required features of an energy efficient routing. In DSR, all nodes except the source calculate their link cost, route cost, minimum transmit power; and add route cost and minimum transmit power to the header of RREQ packet.

c) Transmit Power Control

DSR uses fixed transmit power which covers a maximum range of 250m. Therefore a DSR uses the same power to send the packet to nearest node and distant node from sender. This leads to unnecessary energy consumption to send the packet to near nodes. The aim of suitable transmit power level is to reduce the energy consumption and increase the overall network performance. This method requires that each node can record in suitable packet format field the power level, Ptx, used to transmit that packet. In addition, it requires that radio transceiver can estimate received power, Prx. With the knowledge of Ptx and Prx, the generic node is able to estimate the link attenuation [8]. When a node receives a packet from a neighbor, the channel attenuation is simply noted as the difference (in dB) of the transmitted power Ptxand the received power Prx. The minimum power which is required for the transmission of the packet so that it is successfully received by the receiver (Pt) can be calculated by receiving node as-

$$P_t = P_{tx} + P_r - P_{rx} + M \text{ ---------------------------------- (1)}$$

Where, Pr is the minimum power level required for correct packet reception and M is a power margin and interference fluctuations in power level, this make the transmission more reliable.

d) Delay forwarding

In DSR, the nodes calculate the delay time when they receive the first RREQs. Receiving nodes record these RREQs ids (which include the packet source node id and RREQ sequence number) and delay time δ in request_table and rebroadcast them immediately [11]. The waiting time δ is calculated for each first arrived RREQ as

$$\delta = \mu(\frac{P_t}{E_{rk}}) \text{ -- (2)}$$

Where, μ is a factor to adjust delay time. is the residual battery energy of the sender node k.

Small value of μ provides route with less energy efficient and hop-count than large value of μ. is the minimum transmit power between sender node k and receiver node k+1. If the value of δ is small, the possibility of replacing RREQ in the request_table is rare. Because small value of δ indicates small minimum transmit power, large amount of residual battery energy or small minimum transmit power with large amount of residual battery energy, it is not necessary to wait for a long time to get another route with better cost.

e) Algorithm for DSR

Energy Efficient Route Discovery is the mechanism by which a source node S wishing to send a packet to a destination node D [7]. DSR obtains an energy efficient source route with a list of minimum transmit powers to D. Energy Efficient Route Discovery is initiated only when the "initiator” node S is ready to take a attempts to send a packet to "target" node D and does not already know a route to D.

f) Route Request Processing

To discover an Energy Efficient route, a route request packet is broadcasted over the medium at the maximum power of the interface. This is to maximize the connectivity of the route request packet in the network. The route request packet contains a source route, the link energy information for each link in the source route [10], and the power that the route request packet will be transmitted.

g) Algorithm for Target Node

i. The node checks whether RREQ is first arrived by looking up the sequence number and source node id in request_table.

ii. If RREQ is first arrived, the destination node sends a "Route Reply" to the initiator of the route request packet in which it includes the entire source route from the initiator to the destination and the minimum transmit powers for each hop, computes the RREQ waiting time (δ) and store it in EErequest_table with its waiting time till it is expired [6].

iii. If RREQ is not the first, then the node checks its waiting time δ.

iv. If RREQ is not expired, then DSR compares the route cost of this RREQ and route cost of its copy in EErequest_table.

v. If the route cost of the coming RREQ is better than its copy in the request_table, then the destination node replaces the request_table entry for existing RREQ by the coming copies of RREQ. The coming RREQ with the better route cost is not replied to the destination immediately rather it is delayed for δ. If the node receives another copy of RREQ with better route cost, it replaces again [11].

vi. DSR timer checks the expiration time of RREQs based on the δ in request_table and takes the actions.

vii. If the route cost of coming RREQs is not better than their copies route costs in request_table, then the coming RREQs is discarded.

viii. The route reply route is found by reversing the source route in the route request and sending the packet with this source route. Each node on the route forwards the packet to the next node and transmits at the minimum power computed for the link during the route request. In this way the source learns a source route.

IV. EXPERIMENTAL RESULTS

The Experimental evaluation is made for proposed Dynamic Source routing protocol based efficient mobile adhoc network by using NS2. The tabulation values show that the comparison of transmission rate and end to end delay. The proposed method is compared with DSDV and AODV and the results are evaluated. The following table consists of comparison of delay, transmission rate and energy consumption of DSR with existing protocol.

Table 1 COMPARISON OF DSR WITH EXISTING PROTOCOL

	DSDV		AODV		DSR	
Mobile Nodes	Traffic rate (%)	End to End delay (sec)	Traffic rate (%)	End to End delay (sec)	Traffic rate (%)	End to End delay (sec)
15	24	5.1	67	5.3	62	4.8
30	27	5.9	69	6.5	65	5.2
45	28	6.3	70	7.2	67	5.6
60	32	6.7	73	7.9	69	5.9

Table 1 illustrates the comparison of all three methods. The obtained values from simulation result observed that DSR protocol have higher value than other existing protocols. The proposed DSR protocol shows high transmission rate, low delay and energy consumption.

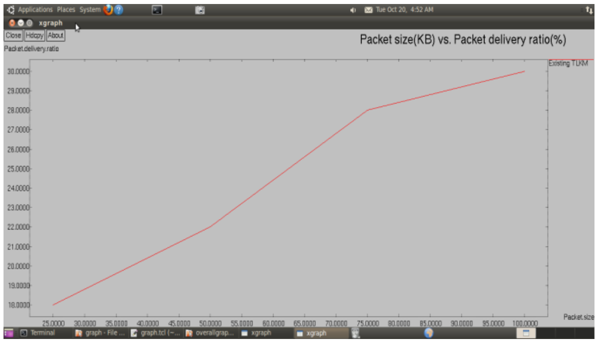

Figure 5. Simulation graph for proposed model

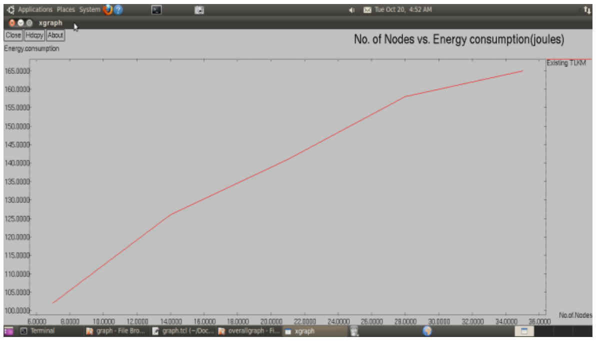

Figure 6. Energy Consumption Simulation graph for proposed model

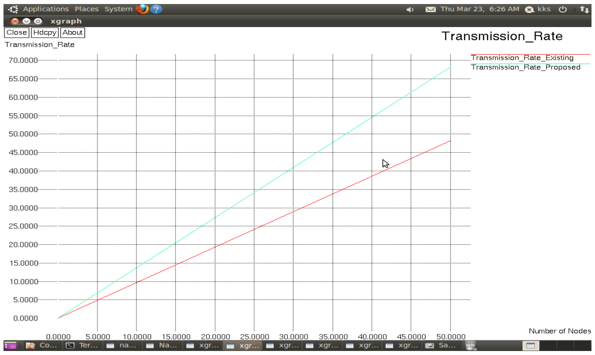

Figure 7. Transmission Rate for proposed model

Figure 5-7 shows the simulation graph for delay, energy consumption and transmission rate. The results are compared with other existing protocols and it shows that the proposed method is more efficient than other approaches.

V. CONCLUSION

Although the state-of-the-art study were realized to the importance of trusting systems efficiency in WSNs and proposed several preliminary solutions, overlooked to EKM techniques, which is perhaps among the most secure route route route key managements. The existing, two-layered method of route route route key management system and a dynamic route route route key update protocol in dynamic WSNs based on the Difie-Helman (DH), respective. However, since each node must exchange the certificate to established the pair-wise route route route key and verify each other's certificate before use, the communication and computation overhead increase dramatically. Here it is unable to access with large size of route route route keys and it increased to the overhead. Here we cannot provide more security. Resolve the route route route key escrow problem. Here presented a certificate less effective route route route key management scheme for dynamic WSNs. In this certificate less public route route route key cryptography the user's full private/public route route route key is a combination of a partial private/public route route route key generated by using a route route route key generation center and the user's own secret and personal value. The special organization of the full private /public route route route key pair will remove the need for certificates and also resolves the route route route key escrow problem by removing the responsibility for the user's complete private/public route route route key. We also take the advantage of of ECC route route route keys defined on an additive group of a 160-bit length as secure as the RSA route route route keys with 1024-bit length.

REFERENCES

[1] Lu, S., Li, L., Lam, K.Y. and Jia, L., 2009, December. SAODV: A MANET routing protocol that can withstand black hole attack. In Computational Intelligence and Security, 2009. CIS'09. International Conference on (Vol. 2, pp. 421-425). IEEE.

[2] Hu, Y.C., Johnson, D.B. and Perrig, A., 2003. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad hoc networks, 1(1), pp.175-192.

[3] Nadkarni, K. and Mishra, A., 2003, November. Intrusion detection in MANETs-the second wall of defense. In

Industrial Electronics Society, 2003. IECON'03. The 29th Annual Conference of the IEEE (Vol. 2, pp. 1235-1238). IEEE.

[4] Patwardhan, A., Parker, J., Joshi, A., Iorga, M. and Karygiannis, T., 2005, March. Secure routing and intrusion detection in ad hoc networks. In Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on (pp. 191-199). IEEE.

[5] Johnson, D., Hu, Y.C. and Maltz, D., 2007. The dynamic source routing protocol (DSR) for Vehicular ad hoc networksfor IPv4 (No. RFC 4728).

[6] Boppana, R.V. and Mathur, A., 2005, December. Analysis of the dynamic source routing protocol for ad hoc networks. In Workshop on Next Generation Wireless Networks (p. 1).

[7] Camp, T., Boleng, J. and Davies, V., 2002. A survey of mobility models for ad hoc network research. Wireless communications and mobile computing, 2(5), pp.483-502.

[8] X. Yu and Z. Kedem. “A Distributed Adaptive Cache Update Algorithm for the Dynamic Source Routing Protocol”, In Proceedings of the 24th Joint Conference (INFOCOM 2005) of the IEEE Computer and Communications Societies, Vol. 1, pp. 730 – 739, 2005.

[9] J. Garrido and M. Marandin. “A Link Cache Invalidation Mechanism for Dynamic Source Routing (DSR) in Ad Hoc Networks”, In Proceedings of IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1 -5, 2007.

[10] G. Kaosar; A. Mahmoud; T. Sheltami. ”Performance Improvement of Dynamic Source Routing Protocol Considering the Mobility Effect of Nodes in Cache Management”, IEEE International Conference on Wireless and Optical Communications Networks, pp. 1 – 5, 2006.

[11] Shukla; N. Tyagi. “A New Route Maintenance in Dynamic Source Routing Protocol”, In Proceedings of IEEE 1st International Symposium on Pervasive Wireless Computing, pp. 4 – 8, 2006.

[12] Perkins, C., Belding-Royer, E. and Das, S., 2003. Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).

[13] Narra, H., Cheng, Y., Cetinkaya, E.K., Rohrer, J.P. and Sterbenz, J.P., 2011, March. Destination-sequenced distance vector (DSDV) routing protocol implementation in ns-3.In Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques (pp. 439-446). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).