An Improved Efficient Data Transmission using Key Management in Mobile Ad-Hoc Network

Vinitha. R. G
PG Scholar
Department of Computer Science And Engineering
Coimbatore Institute of Technology
Coimbatore, TamilNadu, India

***Abstract*:- Mobile Ad Hoc Networks (MANET) is a system that consists of mobile nodes such as laptops, sensors, etc. interfacing without the assistance of access points, bridges, etc. several research have made in terms of routing, synchronization, bandwidth considerations, power consumption, etc. Our focus is only to concentrate on multipath routing techniques is one of the most challenging issue that occurs due in dynamic topology of ad hoc networks. Based on the network conditions, the routing protocols are selected but it faces some difficulty while selecting the exact protocol. Hence, this paper provides a detail comparison between two routing protocols namely, Ad-hoc On-Demand Multipath Distance Vector Routing (AODV) and Dynamic Source Routing. Finally, the best protocol is selected with high transmission rate, low delay and less energy consumption and implemented in the key management applications and also efficient simple MANET based data transmission module is made with improved efficiency and limited delay.**

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

1. INTRODUCTION

Wireless sensor network (WSN) is widely considered as one of the most important technologies in present generation. It consists of thousands of inexpensive miniature devices capable of computation, communication, sensing and multifunctional wireless sensor nodes, with sensing, wireless communications and computation capabilities. These nodes can communicate over short distance via a wireless medium and cooperate to accomplish a common task .For example, environment monitoring, military applications, and industrial process control. In many WSN applications, the deployment of sensor nodes is performed in an ad hoc fashion without careful planning. Once it deployed, the sensor nodes must be able to organize themselves into a wireless communication network.

Mobile network is a technology that can support voice or data network connectivity using wireless, via a radio transmission solution. The most familiar application of mobile networking is the mobile phone. Mobile Ad hoc NET works popularly called MANETs. An MANET is a collection of independent mobile nodes which communicate with each other through radio waves. If no direct link exists between the source and the sink then multi-hop routing is used i.e. packets are forwarded using various techniques. Mobile Ad hoc Networks (MANET) 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. A mobile ad-hoc network (MANET) is a multi-hop wireless network formed by a group of mobile nodes that have wireless capabilities and are in closeness of each other. MANETs facilitate communication among mobile users in military or civil emergency where fixed infrastructure is infeasible. Most MANETs 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 MANET break frequently. The Dynamic Source Routing (DSR) is one of the widely used routing protocols for MANETs. Because of security is considered to improve its performance when compared to other protocols. In this paper we describes a comparison of various protocols which are used in MANET to overcome several issues faced by network transmission.

This paper also concentrated on key management concept. Key management is the process of administering or managing cryptographic keys for a cryptosystem. It involves the generation, creation, protection, storage, exchange, replacement and use of said keys and with another type of security system built into large cryptosystems, it also enables selective restriction for certain keys..Cryptographic schemes are used to protect both routing information and data traffic. Use of such schemes usually requires a key management service. Key management is also a fundamental security service,by providing and managing the basic cryptographic keying material, fundamentals security services preserving confidentiality, integrity and authenticity. Secure key management with a high availability feature is at the center of providing network security. However, all routing schemes neglect the crucial task of secure key management and assume pre-existence and pre-sharing of secret and/or private/public key pairs.

2. RELATED WORKS

Numerous schemes have been proposed for secure routing protocols, and Intrusion Detection and Response Systems, for ad hoc networksAnandPatwardhan*et.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 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.

Nadkarni*et.al* (2003) proposed misuse detection -based IDS for MANETs. 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 MANET by one of nodes as a malicious one in network [1]. BAODV can be regarded as AODV, which is used in MANET 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.

Johnson*et.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. Camp*et.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.

3. METHODOLOGY

3.1Adhoc 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

1.Route Requests (RREQs) messages are used to initiate the route finding process, 2.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.

3. 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).

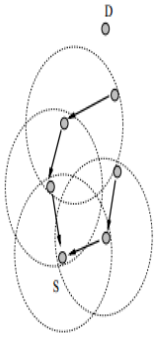


Fig 1 Reverse Path Formation

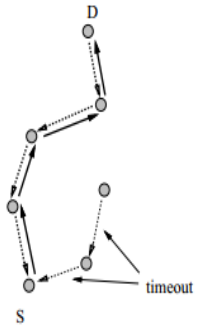


Fig 2 Forward Path Formation

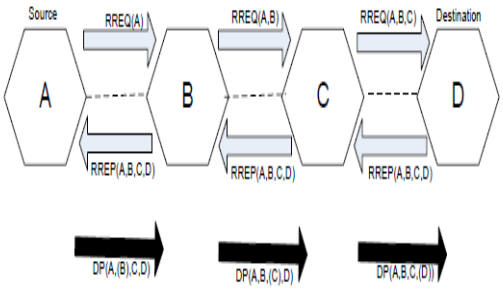
The main difference between DSR and AODV is that the way they keep the information about the routes while in DSR it is stored in the source but while in AODV it is stored in the intermediate nodes. However, the route discovery phase of both AODV and DSR is based on flooding.

3.2 Dynamic Source Routing(DSR)

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. The DSR protocol is a very simple and efficient routing protocol which is used to design for use in multi-hop wireless ad hoc networks of mobile nodes. Each node in the network which maintains a route cache. 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.

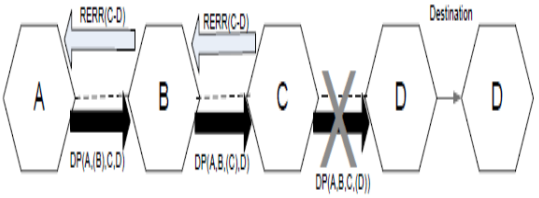
3.2.1. Route Discovery

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.



3.2.2. 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.



3.2.3. 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

3.2.4. 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

$$\delta = \mu\left(\frac{P_t}{E_{rk}}\right)$$

Where, μ is a factor to adjust delay time.

E_{rk} 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.

3.3 Key management

The assessment and study of different types of routing protocols will help in better understanding of the basic characteristics and functioning of the protocols. Analysis of some of the routing protocols can be carried through simulation, using synthetically generated data sets.

Further, there is various mobility models proposed for MANET simulation, it would also be interesting to note the behavior of MANET protocols when subjected to simulation under these models.

1.It aims towards suggesting, designing and implementing a highly efficient security solution for mobile ad hoc networks by establishing secure routing and effective key management mechanism.

2.The proposed protocols should be built upon such a platform that it is not only efficient in terms of meeting the security requirements like message integrity, data confidentiality and end to end authentication but are also cost effective and applicable in practical environment.

Cryptographic schemes are used to protect both routing information and data traffic. Use of such schemes usually requires a key management service. Key management is a fundamental security service, which, by providing and managing the basic cryptographic keying material, fundamentals security services preserving confidentiality, integrity and authenticity. Secure key management with a high availability feature is at the center of providing network security. However, all routing schemes neglect the crucial task of secure key management and assume pre-existence and pre-sharing of secret and/or private/public key pairs. This leaves key management considerations as an open research area in the ad hoc network security field. Conventional key management techniques in MANET may either require an online trusted server or not.

3.4.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. 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.

3.4.1.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.

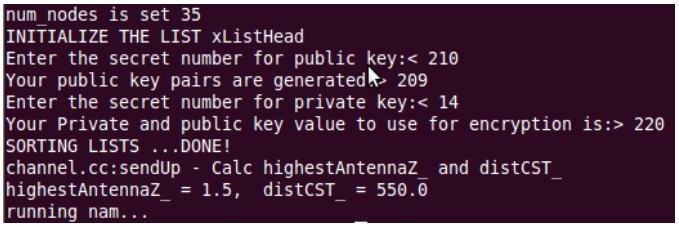
4. EXPERIMENTAL RESULTS

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 DSR and AODV and the results are evaluated. The following table consists of comparison of delay, transmission rate and energy consumption of DSR with AODV protocol.

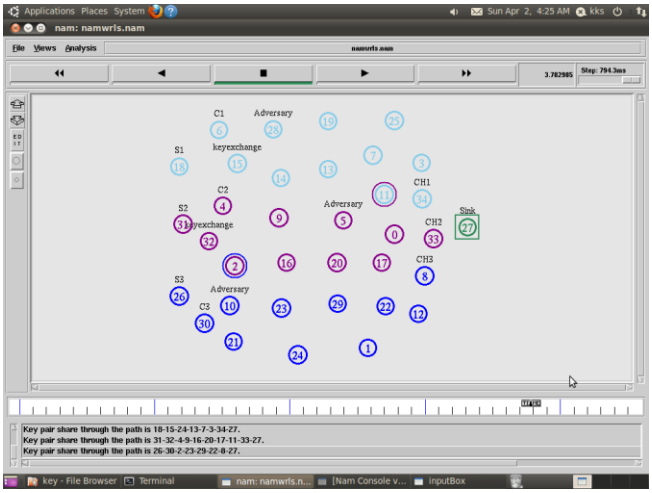
COMPARISON OF DSR AND AODV PROTOCOL

	Efficiency (%)		Traffic rate (%)		End to End delay (sec)	
Mobile Nodes	AODV	DSR	AODV	DSR	AODV	DSR
15	24	25	67	62	5.3	4.8
30	27	28	69	69	6.5	5.2
45	28	30	70	70	7.2	5.6
60	30	31	73	73	7.9	7.9

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.



Terminal shows the public key and private Key



Key management model

BS or Sink can consider a node as compromised if the node disappears for a certain period of time. In that case, the BS must investigate the suspicious node and it can utilize the node fault detection. It is considered to establish the pair wise encryption with a random Key, rather than generating a legitimate master key. One of the Key pair share through the path is 18-15-24-13-7-3-34-27. Sleep scheduling is a widely used and cost effective technique to save energy in WSNs. In order to conserve battery power and to prolong the network lifetime, some sleep scheduling are employed in the networked sensor nodes.In this work, focus has been put on the strategy to address the security issue of MANETs. MANETs have some unique characteristics that make the design of suitable security mechanisms both challenging and interesting. The security issues in MANETs were analyzed.

5. CONCLUSION

Designing of routing protocols for WSNs is the main challenges because of energy efficiency due to the limited energy resources. The energy consumption of the network sensors is dominated by data transmission and reception and routing protocol is designed is to keep the sensors operating for as long time and thus extending the network lifetime. The experimental evaluation shows that high transmission rate, low delay and energy consumption. It is concluded that Dynamic source routing protocol provides a solution to solve routing issues raised by misbehaving nodes with energy efficient and prolong network lifetime when compared to other protocols. The proposed efficient key management and DSR based MANET concept is introduced. Thus, the issue to design and develop an efficient and secure data communication in MANETs is still wide open. Hence, extend this work to achieve best performance. In future, extend this method to implement in real time strategies for processing efficient data transmission.

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] 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.

[4] 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.

[5] 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.

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

[7] 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).

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] 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).