International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 130-133
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

ON THE SELECTION OF ROUTING OPTIMISED KEY DISTRIBUTION TECHNIQUE FOR THE MANET

Gurbax Kaur
Department of Computer Science
Guru Nanak Dev University, Regional Campus
Jalandhar, India

Dr. Jyoteesh Malhotra
Department of Computer Science
Guru Nanak Dev University, Regional Campus
Jalandhar, India

Abstract— **Mobile Ad hoc networks is a collection of mobile nodes that are engage in two way communication on mutual wireless channels. The chief objective of mobile ad hoc network routing protocol is to bring appropriate and effective route establishing between two nodes so that data can be delivered on time. For secure transmission of data key management is a main chunk of any secure communication network. Choosing an appropriate efficient key management technique leads to secure communication protocol. In this paper, a method is created for the distribution of keys which is an enrichment of current technique that is derive on simulation of key management services based on range and mobility profiling in MANET. Key distribution is performed in multi-hop fashion using various levels. The proposed method is named as RET (Ring Expansion Technique). Performance of proposed technique is evaluated with two parameters; routing overheads and remaining energy and these two parameters are checked using different protocols like DSR, AODV, AOMDV and DSDV.**

Keywords— ***Key management, RET, AODV, DSR, AOMDV, DSR***

I. INTRODUCTION

MANET is infrastructure-less network and is built up on demand automatically. It is an arrangement of wireless nodes that are automatically configured on the fly in this manner making it candidate which is reasonable as it is helpful in situations of emergency. In other words it is a network of communication which is multi-hop and temporarily organized with nodes that have transmitters and receivers. The network's topology is dynamic by nature which is made and adjusted on the fly. MANET maintains numerous protocols for routing, for example, AODV (Ad Hoc On-demand Vector Routing), DSR (Dynamic Source Routing), DSDV (Destination Sequenced Distance Vector), OLSR (Optimized Link State Routing protocol), and DYMO (Dynamic MANET On-demand routing protocol). The essential contrast between the MANSET and other networks is the mobility. The traffic of WSN (Wireless Sensor Network) can likewise be relayed over MANET. It implies that communications of WSN are conceivable between various MANET devices [1].

Mobile Ad hoc Network (MANET) [2] is Self-configuring and contains wide range of mobile nodes. The procedure of choosing the topology of the network is known as routing. Capability of devices used in MANET should be of tracing presence of other nodes in the network and take actions to create required set-up to simplify the communication and for sharing services and data. Changes occur in the network traffic routing with the passage of time due to mobility of nodes and protocols to handle traffic routing can be categorized as Proactive and Reactive.

A Reactive protocol also known as On-Demand protocol, routing information is not shared periodically by them. These protocols are used when paths has to be established and maintained only on the demand of the network or when it is required in network. That is done through route discovery. Some of the Reactive protocols are DSR, AODV and AOMDV.

A Proactive protocol also known as Table Driven protocol, In this routing Each node create one or multiple routing table in order to keep the record of information of network topology by rhythmically sharing the network. Every node maintains their tables to keep the record of updated routing information between the nodes present in the network. DSDV is one of the proactive protocols.

In this paper to bring enhancement in key distribution in the network a technique is proposed. Proposed technique is an upgrading of existing technique which was only based on mobility profiling of the nodes. Projected method is concentrated on range of KDC nodes along with the mobility profiling of nodes. A number of routing protocols taken in account to verify which protocol perform better for the proposed technique in relation to routing overheads and remaining energy.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 130-133
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

II. RELATED WORK

Reference [3], BouassidaandBouali presented significant approach for group key management protocol (GKMP) by comparing existing protocols which are DMGSA (distributed Multicast Group Security Architecture), BALADE, GKMPAN (scalable and efficient group rekeying protocol) and Hi-GDH (Hierarchical group key management protocol).Where BALADE and Hi-GDH protocols methods belongs to decentralized strategy, GKMPAN protocol is used for centralized strategy and DMGSA protocol is used for distributed key management strategy. They are compared to explore the requirement for performance evaluation of Group key management protocols in MANETs.

In reference [4], Lin et al created a new protocol for group key management in order to minimize computational and communication overheads rekeying in group caused due to the changes in memberships. Proposed protocol is efficient in to tackle asynchronous and synchronous rekeying operations. To enhance the batch update operations a new algorithm is created with k-node insertion. This protocol is more efficient then ELK, OFT, SKD and LKH in terms of require less computation power, communication bandwidth, efficient when used along binary trees and security with key derivation functions, strong encryption function, etc.

In multi-hop wireless ad-hoc network of mobile nodes DSR is often used, as it is one of the efficient and simplest reactive protocols [5]. The Dynamic Source Routing Protocol is based on source routing, source nodes are one that keeps all the information about hop sequence to reach destination [6]. According to topological changes in the network every node maintains their route cache as DSR permits self-configuring and self-organising network without central administration. DSR protocol has mainly two on-demand modes: 1) Route Discovery and 2) Route Maintenance. To discover and maintain the source route these methods work together on the request of nodes for the transmission of packets to the other nodes [7], [8].

Ad-hoc On-Demand Distance Vector protocol start procedure of discovering route for the destination node only when it has to send data packets to it. For finding the route AODV uses a route discovery algorithm in broadcast configuration and a route reply message is send by the destination node to the source node in unicast way [9]. Sequence-numbers is used in AODV which is maintained by every destination node to reduce the problem of routing loops and routing packets carried-out these sequence-numbers [10]. Tradition route tables are used in AODV to maintain every route per destination. A route table keeps the information of: active node for communication, address of destination node, sequence number, number of hops to reach the destination and termination time [8].

Ad-hoc On-demand Multi-path routing protocol (AOMDV) discovers multiple paths among the source and the destination when source node wants to communicate with the destination node. These multiple routes used as a backup on failure of one route and they also helps in load spreading in network [11].

DSDV is one of the proactive protocols that is table driven routing protocol. Destination-Sequenced Distance Vector Routing protocol is established on Bellman-Ford routing method [12]. Each node has its own sequence-number that is created with every destination which helps to detect a route is how old in DSDV. Route information is updated periodically and the route with a higher sequence-number replaces the old route with lower sequence-number. Emitter generates these numbers and with help of these numbers emitter send out the next updates. It uses additive updates and full dump. With setting time broadcast of route update is delayed [13]. Updates of rote information are periodically transmitted. Decayed rotes and entries are deleted on next hops [13], [14].

III. DESCRIPTION OF PROPOSED TECHNIQUE (RET)

In the **existing** key distribution technique KDC's are selected on the basis of contextual mobility profiling [15]. Management node contains the mobile profile vector which consist all the updates of node status that is called as profile manager [15]. Basically there are four kind of status of the nodes in the network according to their mobility and these are 1.Stationary (ST): Stationery nodes are those which remain at the same position throughout the simulation, 2.Relatively stationary (RS): Relatively stationery nodes are those which changes there position very slowly during simulation, 3.Mobile (MB): Mobile nodes change their position during the simulation and 4.Highly mobile (HM): Highly mobile nodes are those which changes their position very fast than mobile nodes. According to the status of nodes root node select only ST and RS nodes to make them KDC's for further distribution of keys among the nodes present in the network.

A technique is **proposed** with the aim of significantly reduce the routing overheads and to increase the remaining energy of existing key distribution technique and technique is named as Ring Expansion Technique (RET). Nodes present in the network are selected as Key Distribution Centre's in ring expansion manner on the bases of ranking mechanism which depends upon the signal strength, mobility, power and range of the nodes. In the proposed work process of selecting KDC's take place in the levels in ring expansion manner. Where a small range is set for every node working as KDC's to search for the ST and RS nodes.

In Level1: A ST node is selected randomly from network on the bases of ranking mechanism from all the nodes as root node then which is made a KDC.

In Level2: In this level root node working as Key distribution centre search in its region for ST and RS nodes and make them KDC's.

In Level3: In this level selected KDC's of previous level searches in their respective regions for ST and RS nodes to make them KDC's.

This process of searching nodes to make them key distribution centres will continue for the entire network. The proposed

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 130-133
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

technique makes process key distribution more efficient, less time consuming, saves more remaining energy and effectively reduces the routing overheads.

IV. PERFORMANCE ANALYSIS

Analysis of performance of ring expansion technique in comparison to existing technique can be seen in sections mentioned below:

A. Performance Matrices –

Routing overheads and remaining energy are two performance metrics used to measure the performance of RET. Where these parameters are evaluated using different routing protocols. Experimental results are calculated among routing overheads vs. routing protocols and remaining energy vs. routing protocols for comparing the performance of existing and proposed techniques. Routing overheads of a network is calculated by fraction of no. of control packets sent by source node vs. no. of data packets received by destination node. Large amount of energy is consumed in network while simulations are performed and aim of every technique is to save energy as much as possible. Initial energy is constant in RET that is 30 joules.

B. Simulation Environment

Simulations are performed in NS2.345 simulation tool using VMware workstation on IEEE 802.11 MAC layer, Random waypoint Mobility model, network size is 20 nodes and window8 is used. 400*400 m2region is used for performing simulations. Initial energy is 30 joules. Where nodes move with different speed (m/s) and move independently in the network figure (1).

SIMULATION ENVIRONMENT	
NAME	VALUE
Channel Type	Wireless Channel
Propagation	Two Ray Ground
N/W Interface Type	CMU PriQueue
Protocol	DSR
Antenna	Omni Antenna
NO. of Nodes	20
MAC	IEEE802.11
Simulation Area	400*400 m*m
Initial Energy	30 Joules
Node Speed	0,2,5ms

Fig. 1. Simulation Environment

C. Results and Analysis

Protocols: Different protocols are used such as reactive like DSR, AODV and AOMD and proactive protocols like DSDV to measure the performance of proposed technique against current technique in terms of routing overheads figure (2)and remaining energy figure(2).

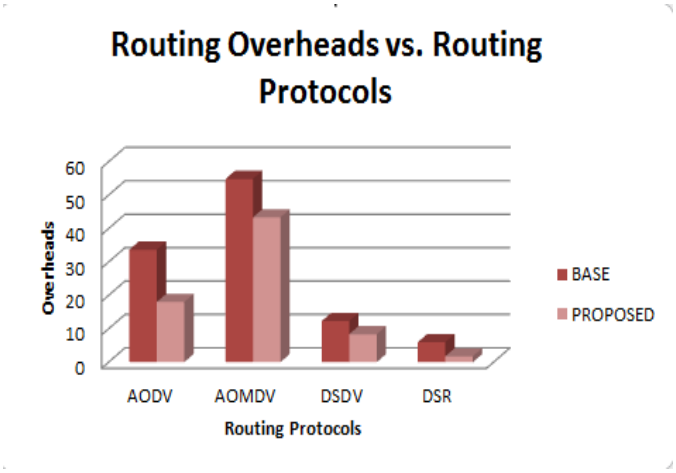

Fig. 2. Routing Overheads vs. Routing Protocols

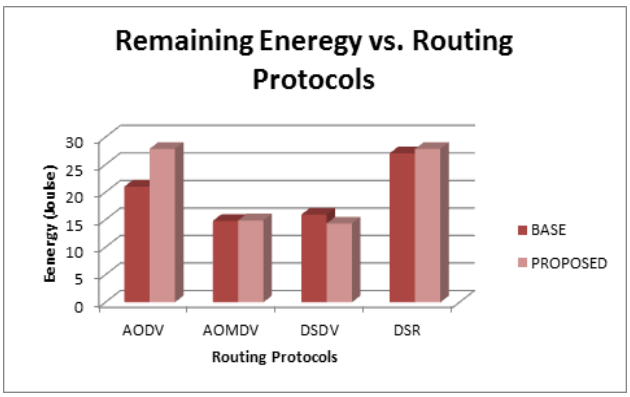

Fig. 3. Remaining Energy vs. Routing Protocols

V. CONCLUSION AND FUTURE SCOPE

This research work is done with the aim to reduce the routing overheads and to save energy while performing key distribution process, which is significantly achieved. This technique also reduces simulation time. Different protocols were used to evaluate the performance of proposed work. From results we can conclude that performance of DSR protocol is much more effective than the other protocols for this technique. In order to further enhancements in the proposed technique concept of clustering can be embedded in it.

peak signal to noise ratio of performance of our proposed method of watermarked image and original image with various watermark image, where our watermarked images peak signal to noise ratio has a better performance than others.

VI. REFERENCE

[1] C. Krishna Priya, Prof. B. Satyanarayana, "A Review on Efficient Key Management Schemes for Secure Routing in Mobile Ad Hoc Networks", International Journal of Computer Engineering and Applications, Vol. V, Issue I, January 2014.

[2] C. E. Perkins and E. M. Royer, "Ad-hoc on demand distance vector routing," in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), vol. 3, New Orleans, LA, USA, February 1999, pp. 90–100

[3] M. S. Bouassida and M. Bouali, "On the performance of groupkeymanagement protocolsinMANETs,"inProceedings of the Joint Conference on Security in Network Architectures and Information Systems (SAR-SSI '07), pp. 275–286, Annecy, France,June2007.

[4] J.-C. Lin, K.-H. Huang, F. Lai, and H.-C. Lee, "Secure and efficient group key management with shared key derivation," Computer Standards & Interfaces, vol. 31, no. 1, pp. 192–208, 2009.

[5] G. Jose Moses, D. Sunil Kumar Prof.P.Suresh Varma N.Supriya, " A Simulation Based Study of AODV, DSR, DSDV Routing Protocols in MANET Using NS-2," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, March 2012 ISSN: 2277 128X .

[6] Satveer Kaur, "Performance Comparison of DSR and AODV Routing Protocols with Efficient Mobility Model in Mobile Ad-Hoc Network," IJCST Vol. 2, Issue 2, June 2011.

[7] RajeshDeshmukh,AshaAmbhaikar, "Performance Evaluation of AODV and DSR with Reference to Network Size," International Journal of Computer Applications (0975 – 8887) ,Volume 11– No.8, December 2010.

[8] V.K.Taksande,Dr.K.D.Kulat, " Performance Comparison of DSDV, DSR, AODV Protocol with IEEE 802.11 MAC for Chain Topology for Mobile Ad-hoc Network using NS-2," IJCA Special Issue on "2nd National Conference-Computing, Communication and Sensor Network" CCSN, 2011.

[9] Prof.S.P.Setty, Narasimha Raju K, Naresh Kumar K, "PERFORMANCE EVALUATION OF AODV IN DIFFERENT ENVIRONMENTS," International Journal of Engineering Science and Technology,Vol. 2(7), 2010, 29762981.

[10] Nilesh P. Bobade, Nitiket N. Mhala , "Performance Evaluation of Ad Hoc On Demand Distance Vector in MANETs with varying Network Size using NS-2 Simulation," (IJCSE) International Journal on Computer Science and Engineering,Vol. 02, No. 08, 2010, 2731-2735.

[11] V. C. Patil, R. V. Biradar, R. R. Mudholkar, S. R. Sawant, "On-demand multipath routing protocols for mobile ad hoc networks issues and comparison", International Journal of Wireless Communication and Simulation, Vol. 2, No 1, pp. 21-38, 2010.

[12] Arun Kumar B. R., Lokanatha C. Reddy, Prakash S. Hiremath, "Performance Comparison of Wireless Mobile AdHoc Network Routing Protocols," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008.

[13] Abdul Hadi AbdRahman ,Zuriati Ahmad Zukarnain, "Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks," European Journal of Scientific Research ISSN 1450-216X Vol.31 No.4 (2009), pp.566-576.

[14] Amith Khandakar, "Step by Step Procedural Comparison of DSR, AODV and DSDV Routing protocol," 2012 4th International Conference on Computer Engineering and Technology (ICCE 2012) IPCSIT vol.40 (2012).

[15] Shaftab Ahmad and Syed Zubair Ahmad, 2006. "Contextual mobility profiling secure routing infrastructure for mobile ad hoc networks.", Presented in HONET 2006. Bahria University & M. A.Jinnah University Islamabad, Pakistan.