International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 6, ISSN No. 2455-2143, Pages 88-91
Published Online in IJEAST (http://www.ijeast.com)

A NOVEL QOS AWARE KEY DISTRIBUTION TECHNIQUE FOR 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— **A mobile ad hoc network (MANET) comprises of accumulation of nodes which are independent and communicate with one another by using a wireless network which is multi hop. Majority of the cryptosystems are based on the efficient, robust, and secure system for management of key. Key management is very crucial task in MANET and key management is necessary because key management is an important fraction of any secure communication. MANET is vulnerable to attacks as transmission is done through wireless medium that can be interfered and mistreated by intruder. In this work, a hierarchy is created for the distribution of keys which is an enhancement of existing technique that is based on simulation of key management services in MANETs using mobility profiling by considering the range of key distributor and dividing the key distribution process into various significant levels in multi hop fashion. The proposed hierarchy is named as Ring Expansion Technique. The parameters which are taken into account are energy consumption and routing overheads and these parameters are checked with the variations in mobility of node and by taking different number of nodes.**

Keywords— **MANETs, Key management, Ring Expansion Technique, KDC**

I. INTRODUCTION

Previously there was a mainframe computer which is centrally located with terminals for various clients, as of now there is one or more than one computer for every individual. Be that as it may, we are moving to the age of Ubiquitous Computing, in which one individual will have numerous gadgets accessible in his or her surroundings (i.e., personal digital assistants, handheld digital devices, laptops or cell phones etc.) and where power of computation will be accessible all over the place. The quality of devices of communication and ubiquitous computing makes remote systems a key answer for their collaboration. Consequently, the arena of wireless communication is developing to meet distinctive difficulties. Without a doubt, the most requested administration by versatile clients is connections of network and relating information administrations. The majority of the current associations among these devices which are wireless are based on infrastructure gave by private networks or providers of service. Base stations are utilized to interface remote systems to the "outside" world. A cell phone is inside a network which is having wireless interfaces with the nearest base station that is inside its radius of communication. As the versatile unit moves out of the range of a base station into another's reach, the connection of portable unit is given from the old base station to the new one, and the mobile device can proceed with correspondence of course. Office Wireless Local Area Networks (WLANs) are regular uses of this sort of system incorporate giving the required system administrations when the required systems administration bases are not accessible in a given zone is a genuine test. [1]

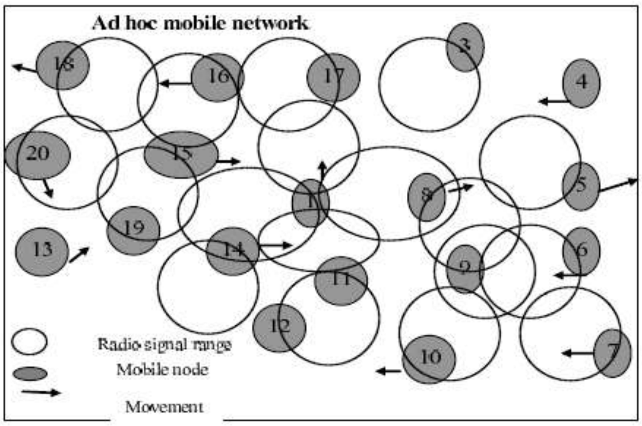


Fig. 1. MANET with dynamic mobile nodes [1]

MANETS (Mobile ad-hoc networks) provide advantageous communication which is free of infrastructure over a shared wireless medium which is wireless. MANETs are additionally viewed as a perfect technology for making networks of regular communication for applications related to military and civilian. As of late, MANETs have obtained a lot of consideration in both industry and academia. This developing technology intends to offer services of networking "anytime-anywhere" on a large scale conceivably. The users of MANET which are nodes hope to communicate seamlessly and securely among them and in addition with whatever are left of the Internet globally. [2]

For accomplishing the high security in MANET, distinctive schemes of Key Management are utilized. Utilizing and overseeing keys for security is a significant assignment in MANET because of its operations which are constrained of energy, dynamic topology, variable links of capacity and limited physical security. Diverse keys of cryptography are utilized for encryption like public key, symmetric key, group key and hybrid key (symmetric key + asymmetric key). [3] If the key size is large, the corresponding cryptographic algorithm ensures a guaranteed secure communication, but lead to more energy consumption. Hence energy efficient key management techniques are used in wireless networks. Secure and efficient key management in ad hoc networks [4]

II. Related Work

In Paper [8], authors ChangandKuo projected a approach for multicast MANETs known as two-step secure authentication approach. A Markov established a chain trust model which to check the Trust Value (TV) of the nodes and the node among other nodes having highest trust value is chooses as certification authority server. Various analyses performed for guarantying the security in this method which is and the outcomes was positive that this method provides reliable, secure authentication in multicast MANETs. The trust value method is very near to perform simulation under vast variety of situations is analyses through numerical results of TV. In TV the speed of convergence is independent of the trust classes and initial values.

Paper [5] HuangandMedhi to enhance the survivability and scalability of the group management strategy for wide scale WAN have proposed a secure group key management strategy. This multi-level security strategy was proposed using decentralized approach of group key management and multilevel security model. This strategy efficiently improves spirited to single point failure problem and minimizes overheads of key management.

In this paper B.Madhusudhanan, S.Chitra and C.Rajan [6], proposed a key management technique for multicast security based on concept of mobility in MANET. On the bases of nodes link mobility and availability nodes are categorized according to stability index. A multicast tree is designed in such a way that a strong node is associated to every weak node in the network. For data transit in multicast tree the encryption technique used is a session key based encryption. Initiator node is responsible for periodic rekeying process. Where rekeying time interval is constant which significantly reduces the keying overheads. This technique efficiently minimizes packet drop rate and increases the data security.

III. Description Of Proposed Key Distribution Technique (Ret)

In **base work** for choosing appropriate nodes to make a key distribution configuration whose shape and size changes dynamically with a section of time, contextual mobility profiling [7] is used. The mobile profile vector keeps the record of dynamic changes in the status of nodes. Basically there are four kind of node status which according to their mobility:

i. If a node is moving with speed >= 0.5 m/s and speed < 2 m/s a status of node will be “RS”.

ii. If a node is moving with speed >= 2 m/s and speed < 6 m/s a status of node will be “MB”.

iii. If a node is moving with speed >= 6 m/s then status of node will be “HM”.

Above mentioned mechanism is used for ranking the nodes on the bases of computation capacity, node behaviour, mobility and power transmission range etc. according to the current status of nodes in profile vector status [7].

Fields like battery power, average mobility, device category, average no of nodes priority factor, signal strength also include in the profile vector. In the existing work during simulation, the target is to trace stationery or relatively stationery nodes because the keys should be distributed in only these nodes in a base scenario. On the other hand mobile and highly mobile nodes are not considered for the key distribution process. The tool used NS-2 version 2.27 on windows XP operating system for the simulations [8]. This technique efficiently reduces the traffic in network plus increases the performance and network security.

In the **proposed work**, the main aim is to reduce routing overheads and also energy consumption. In the work already existing, in which there is root node which is normally stationary node and selected as an initial key manager or KDC. It assigns other nodes for dissemination of key via mechanism of ranking dependent upon different properties such as strength of signal, power and mobility. But in existing method routing overheads are more because root node has to send data to all other nodes which are present in the network individually. There was more energy needed to maintain links among root node and all other nodes in the network. Time consumed for simulations was more. In the proposed scheme, the hierarchy is created for efficient key distribution named Ring Expansion Technique (RET).

RET is an enhancement of existing technique of key distribution based on simulation of key management services in MANETs using contextual mobility profiling [7]. In ring expansion technique work is focused on range of key distribution centre along with contextual mobility profiling. The key distribution process takes place in ring expansion manner using multi hop technique. Key distribution process is done in various significant levels.

Level 1: Initially a stationary node is randomly selected as a root node from all the nodes present in the network and that node is selected as KDC.

Level 2: In level (2) the root node will trace a small portion of network in ring expansion manner to find out the stationary or relatively stationary nodes present in its range. Now, these stationary and relatively stationary nodes will be selected as KDC's.

Level 3: In level (3) now, these KDC's will trace further small portion of the network in ring expansion manner to find out the stationary and relatively stationary nodes present in their respective range. These nodes will be selected as KDC's.

This ring expansion technique is followed for the selection of KDC's to distribute keys to all nodes until the whole network is covered. The keys are distributed in the range which is very limited which leads to better quality of link. In this way, routing overheads gets reduced and also energy consumption gets decreased. The parameters which are considered here are routing overheads and remaining energy. These parameters are checked with mobility and scalability.

IV. Performance Analysis

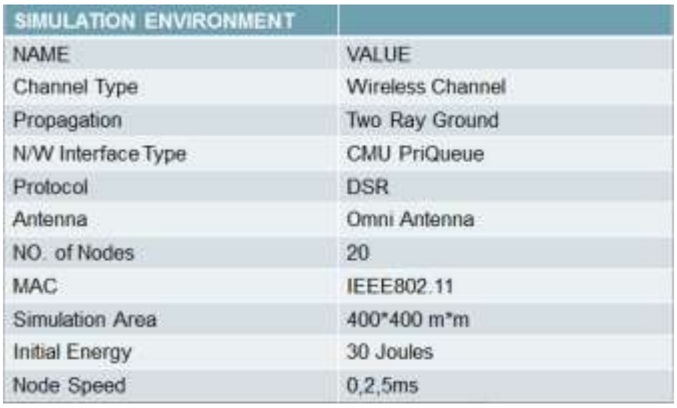
Performance of the proposed ring expansion technique has been evaluated and outlined in the below mentioned subdivisions:

A. Performance Matrices

Performance metrics used to appraise our proposed technique are routing overheads versus mobility, remaining energy versus mobility, routing overheads versus no. of nodes, and remaining energy versus no. of nodes. Where routing overheads is the ratio of number of control packet sent to the number of data packets received. Comparison is done for evaluating routing overheads in base vs. proposed technique Mobile ad-hoc network requires the large amount energy for routing, communication, key distribution and maintain links in the network etc. Every technique is proposed with an aim to reduce the overheads and to save the energy in order to make their proposed work more efficient and reliable. In our proposed work initial energy is fixed 30 joules and comparison is done for energy saved that is remaining energy in base vs. proposed technique.

B. Simulation Environment

Performance of proposed technique is examined using simulation tool. Figure (2) shows the simulation setup that is network environment. The proposed technique is simulated in NS2.345 on window8. Simulation environment of this protocol is VMware workstation. We use IEEE 802.11 as MAC layer. In our simulation mobile nodes move in a 400*400 m2 region. Mobility model is considered here as random waypoint. It is assumed that each node moves independently with the different speed (m/s). Network size is varied as 20, 30 and 40 nodes. Initial Energy used is 30 joules.



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. 2. Simulation Environment

C. Results and Analysis

The parameters considered in the simulation are Routing Overhead and Remaining energy. These two parameters are checked against different number of nodes and variations in mobility of nodes.

1. **Mobility:** Mobility is the speed with which nodes move in the network. In MANET speed varies depending upon applications. Commercial applications which are of short range network so, speed of network is high, military applications are long range network therefore speed of network is low. Speed is inversely proportional to range of network. With increase in speed of nodes, efficiency of key distribution decreases and with decrease in speed of nodes, efficiency of key distribution increases. Routing overheads and remaining energy parameters are evaluated using the different mobility speed of nodes (6ms, 12ms and 18ms) as shown in figure (3) and figure (4).

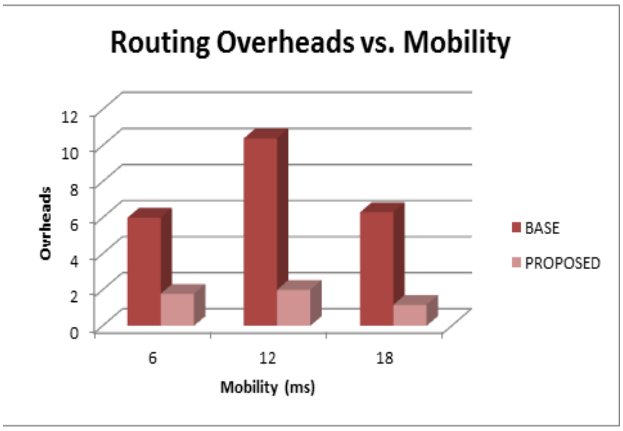


Fig. 3. Routing Overheads vs. Mobility

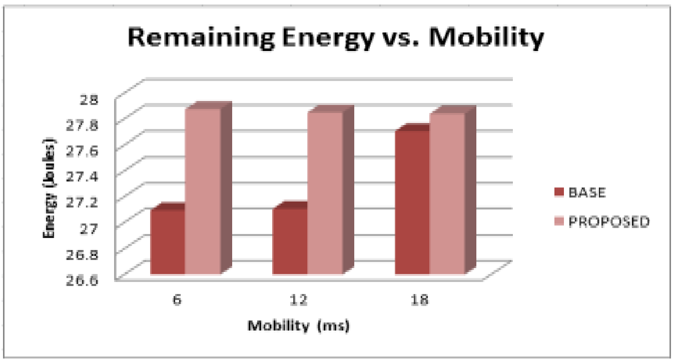


Fig. 4. Remaining Energy vs. Mobility

2. **Number of Nodes:** In the proposed key distribution technique with increase in the no. of nodes the key distribution becomes more efficient; denser the network more efficient will be the key distribution. In RET routing overheads reduces and remaining energy efficiently increases as shown in figure (5) and figure (6). The results are evaluated for scalability of base and proposed technique by varying the size of network from 20, 30 and 40 no. of nodes.

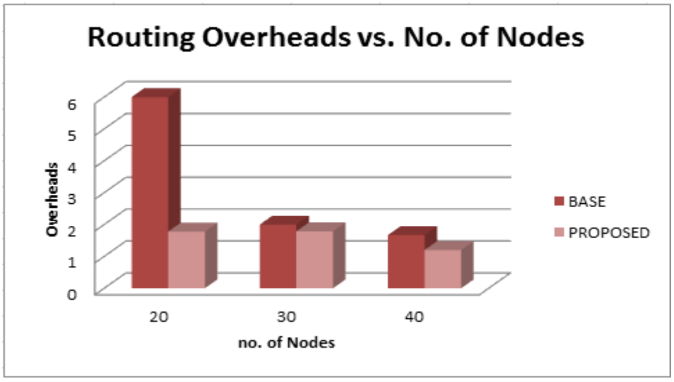


Fig. 5. Routing Overheads vs. No. of Nodes

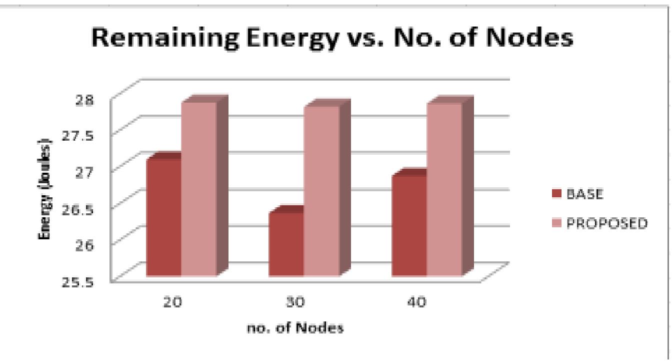


Fig. 6. Remaining energy vs. No. of Nodes

V. CONCLUSION AND FUTURE SCOPE

The main aim of this research is to propose a technique for key management so that minimize the routing overheads and increase the remaining energy. Where with this technique simulation time is also reduces significantly. In proposed ring expansion technique selection of KDC's is performed in levels with the only limited range in multi-hop fashion. In future this scheme can be enhanced by using the concept of clustering for the further improvements.

VI. ACKNOWLEDGMENT

The main aim of this research is to propose a technique for key management so that minimize the routing overheads and increase the remaining energy. Where with this technique simulation time is also reduces significantly. In proposed ring expansion technique selection of KDC's is performed in levels with the only limited range in multi-hop fashion. In future this scheme can be enhanced by using the concept of clustering for the further improvements.

VII. REFRENCES

[1] Their Khdour, Abdullah Aref, "A Hybrid Schema Zone-Based Key Management for MANETs", *Journal of Theoretical and Applied Information Technology,* Vol. 35, No. 2, January 2012.

[2] Kyung Hyune Rhee, Young-Ho Park, Gene Tsudik, "A Group Key Management Architecture for Mobile Ad-Hoc Wireless Networks", Journal of Information Science and Engineering, 21, 415-428, 2005.

[3] Renu Dalal, Yudhvir Singh, Manju Khari, "A Review on Key Management Schemes in MANET", *International Journal of Distributed and Parallel Systems (IJDPS),* Vol. 3, No. 4, July 2012.

[4] Bing W., et al., "Secure and efficient key management in mobile ad hoc networks", *Journal of Network and Computer Applications, Elsevier Publications*, 2007, Volume 30, pp. 937-954.

[5] B.-J.ChangandS.-L.Kuo,"Markov chain trust model for trust value analysis and key management in distributed multicast MANETs,"*IEEE Transactionson Vehicular Technology*,vol.58, no.4,pp.1846–1863,2009

[6] D. Huang and D. Medhi, "A secure group key management scheme for hierarchical mobile Ad hoc networks," *Ad Hoc Networks*,vol.6,no.4,pp.560–577,2008.

[7] B.Madhusudhanan, S.Chitra and C.Rajan, ''Mobility Based Key Management Technique for Multicast Security in Mobile Ad Hoc Networks",*Hindawi Publishing Corporation □e Scientific World Journal* Volume 2015.

[8] 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.