International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 5: May 2016, pp 17-20. www.aetsjournal.com ISSN (Online) : 2394 -6237

A Multilevel Distributed Key Management for MANETs

Pawandeep kaur jhajj, Jaspreet kaur

Abstract— In this paper, A new multi-level Key Management System for MANET based systems is presented. The multilayer key management system for Mobile Ad-hoc Networks which can provide higher energy efficiency and a heiriarchical design which can extend the MANET to a very large networks and still providing connectivity and high energy efficiency and key management has been developed.

Keywords— *Distributed Key Management, MANET*

I. INTRODUCTION

Mobile Ad hoc Networks or MANETs are the group or cluster of mobile devices like smart-phones, laptops, intelligent devices etc. which have created an ad hoc or infrastructure less and wireless network in which any device can join or leave the network anytime. The network is self configuring. The network is created to communicate information when there is no source of infrastructure communication like WLAN or LAN etc. One of the applications of such MANETs is E-Class in which a professor conducting the class (generally a tutorial) can allow students to take the class while sitting around the campus without having them to be present in the classroom. The students with their mobile devices e.g. Laptops or smart phones, can join the ad-hoc network and take the tutorials which is a multi-cast communication. The professor sends the questions in multi-cast form and students reply back their answers in form of one to one communication. For the system to keep forward and backward (archived) secrecy, re-keying the communication is necessary every time a student joins or leaves the network. Thus key management becomes a very important part of such secure classes. Many challenges are existing in generating and maintaining keys as nodes are mobile and have limited battery capacity, the energy sent by each node transmitting the data is a valuable resource and has to be efficiently used for network management operations such as key distribution. In the case where the multi-cast group is dynamic, the valid members of multi-cast group need to be updated with new keys after every membership changes so that new members do not access past data(backward secrecy) and departing members do not access future transmission(forward secrecy). The GC has to transmit every updated keys after a membership change. To overcome these challenges a new concept of key management developed over the idea of hierarchical key management scheme of MANETs. A method of multilayer Key Manager has been proposed wherein, each key manager can generate new KEKs which are signed by Global Key Managers in order to verify the concept. By distributing the key generators and using this concept one can develop a network which can be extended for 100s of nodes having a secure communication and high energy efficiency can be maintained.have The simulation is developed for testing the proposed scheme on MATLAB which is very great tool for simulation and algorithm prototyping. A test bed is developed in which the nodes are deployed over an area and then form a tree based hierarchy using k-NN clustering approach. The value of 'k' defines the value of 'm' in m-ary tree. i.e. if 'k' is 2 the tree becomes a binary tree and so on. Then the idea is tested by sending traffic over network and energy consumption and delay like parameters are tested.

Pawandeep kaur jhajj, Mtech Student, Department of ECE, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib,India. (Email: jhajj_pawan@yahoo.in)

Jaspreet kaur, Assistant Professor, Department of ECE, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib,India. (Email: Jaspreet.kaur@bbsbec.ac.in)

II. RELATED WORK

Verma et al. in [1] propose a secured, energy aware key establishment and distribution scheme. The secure group key management also includes techniques for managing the group keys when a member leaves or joins the group. The emphasis is given to design the key distribution and re-keying protocol with very low communication overhead.

Dhillon et al. in [2] describe this approach in which a PKI is tightly coupled with an OLSR MANET at the network layer level and the OLSR control packets are leveraged to support various security related activities as well. They have implemented a fully distributed CA (certificate authority) and integrated it with an existing implementation of OLSRv4 (OLSR for IP version 4) Intricate details of their implementation are presented to develop insights into the key aspects of the proposed solution.

Boneh et al. in [3] propose a fully functional identity-based encryption (IBE) scheme. The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Diffie--Hellman problem. Their system is based on bilinear maps between groups. The Weil pairing on elliptic curves is an example of such a map. They give precise definitions for secure IBE schemes and give several applications for such systems.

Umaparvathi et al. in [4] presents a comparison of the most commonly used symmetric encryption algorithms AES (Rijndael), DES, 3DES and Blowfish in terms of power consumption. A comparison has been conducted for those

encryption algorithms at different data types like text, image, audio and video. Experimental results are given to demonstrate the effectiveness of each algorithm.

Martin et al. in [5] examine the performance of the new cipher in MANET and wireless LAN networks and make a performance comparison with that of AES. Since 1970s, data encryption standard (DES) has received a substantial amount of attention from academic cryptanalysts. However, in 1998 it has been proved insecure and on October 2000, National Institute of Standards and Technology (NIST) announced that the Rijndael algorithm has been selected as the advance encryption standard (AES).The algorithm is based on AES.

Jung et al. in [6] considers energy constrained routing protocols and workload balancing techniques for improving MANET routing protocols and energy efficiency. A new routing protocol is given that employs adaptive load balancing technique to the MANET routing protocols with node caching enhancement. Also, it shows new application of energy efficiency metrics to MANET routing protocols for energy efficiency evaluation of the protocols with limited power supply. Our contributions include: (i) New energy efficient AODV-based node caching routing protocol with adaptive workload balancing (AODV-NC-WLB); (ii) New application of energy efficiency metrics to MANET routing protocols; and (iii) An implementation and simulation study in NS-2 of energy efficient AODV-NC-WLB sustaining considerable improvement in throughput, overhead, delivery ratio and delay over the standard AODV for high work load scenario.

Zhang et al. in [7] propose a probabilistic approach that dynamically adjusts the rebroadcasting probability as per the node distribution and node movement. This is done based on locally available information and without requiring any assistance of distance measurements or exact location determination devices. They evaluate the performance of our approach by comparing it with the AODV protocol (which is based on simple flooding) as well as a fixed probabilistic approach. Simulation results show their approach performs better than both simple flooding and fixed probabilistic schemes.

Eschenauer et al. in [8] present a key-management scheme designed to satisfy both operational and security requirements of DSNs. The scheme includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication capabilities. It relies on probabilistic key sharing among the nodes of a random graph and uses simple protocols for shared-key discovery and path-key establishment, and for key revocation, re-keying, and incremental addition of nodes. The security and network connectivity characteristics supported by the key-management scheme are discussed and simulation experiments presented.

Capkun et al. in [9] propose a fully self-organized public-key management system that allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services. Furthermore, their approach does not require any trusted authority, not even in the system initialization phase.

Du et al. in [10] propose a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. They show that the performance (including connectivity, memory usage, and network resilience against node capture) of sensor networks can he substantially improved with the use of their proposed scheme. The scheme and its detailed performance evaluation are presented in this paper

III. Proposed Work

In this proposed work, A multilayer hierarchical key management system is developed for Mobile Ad-hoc networks. In such a network, the mobile nodes are connected in a hierarchical manner and the Key Manager is not a single object. Instead, in this work, the key managers are distributed into 't' managers and in order to save the energy, these key managers perform distributed key generation and these keys are only used to encrypt the key generated by lower level distributors. This way, these distributed generated KEKs are highly secure as it need at least 't' generators to verify the signature making it highly secure. Secondly, each level has got authenticated by a minimum of 't' master key generators and thus a lower level key generator can be trusted easily as verified. For each level, to create a new key generator, it requires a minimum of 't' key generator above this level to verify the authenticity.

Such a system can be extended to 100s of nodes without worrying about a node leaving the system at any level. This is possible because key generation is distributed and as long as 't' generators are available at upper level, this system can generate and verify the key. Further, to restrict future communication for a given node, only thing needed is re-keying the 'n-1' level parent node everything else will work perfectly

IV. Experimental Set Up

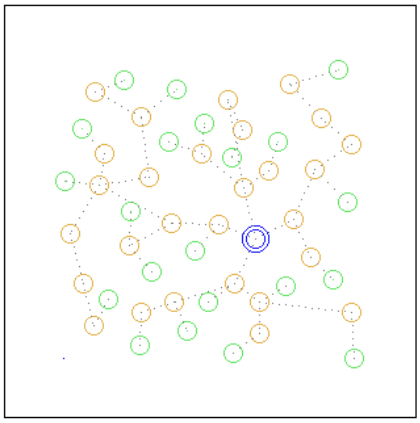

Figure 1: Simulation of '50' node generation. Double Circle node is Master Node.

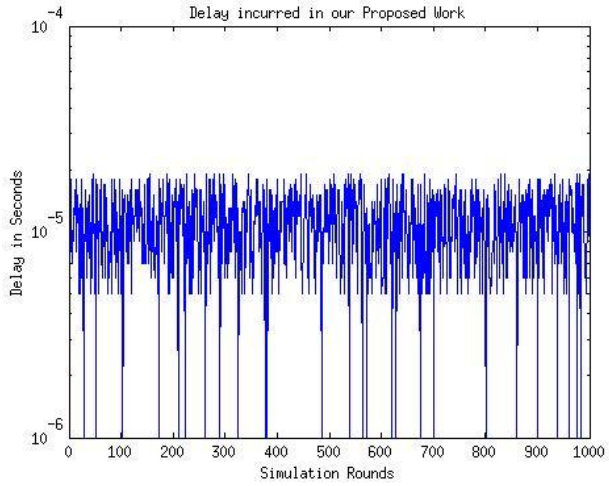

Figure 2: Delay incurred in each round. This have 1000 rounds of simulation

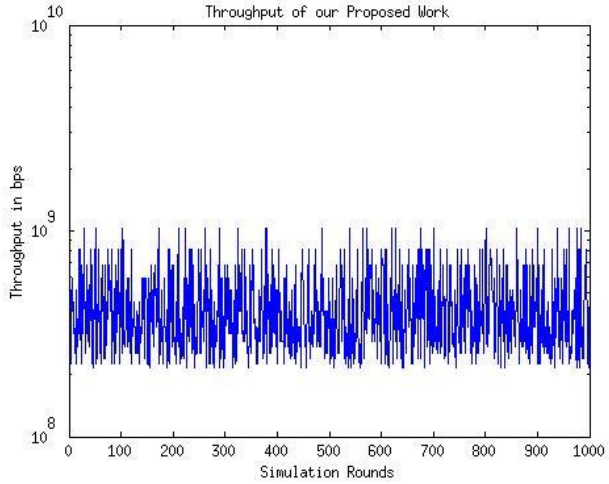

Figure 3: Throughput required for each round when a request is processed.

This experimental simulation in MATLAB is developing as it is a great tool for testing simulation which require vector algebra as it is natural at it.

This work included development of a test bed which can generate 'n' number of nodes and compute 'k' nearest nodes in order to form a tree structure. Further, these nodes can transmit packets by following the chain created. The code for it has been written using 'struct' element as definition variable for nodes, packets and simulation environment. Further the figure 1 shows a test generation of 50 nodes wherein, a node with two concentric circles is master node

Then the concept of multi-key generation is applied by simulating it. In this simulation, it has been assumed that 'n' number of random requests for joining as well as leaving the network. This is the case where the efficiency of a key manager comes into play. The number of nodes affected by leaving or joining of a node is solely based on number of siblings it has and number of children it has (if any). These values are then computed using an arbitrary randomization equation. This equation says that when a node leaves the network, the number of nodes connecting and leaving the network will affect the number of partitions of the tree. Each partition will have 'm' levels based on the initial 'k' defined for this 'k-ary' tree. This will then suggest that the request has to be processed from n new nodes (leaving or joining) and k*m nodes affected by this partition. Such system will allow us to define the traffic generated and the delay incurred based on the levels.

The results can be best read in terms of probability distribution assuming a 'Normal' distribution computed using the results of simulation.

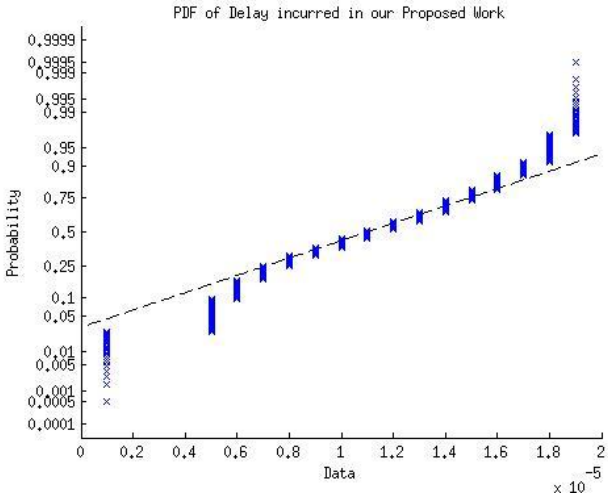

Figure 4: Probability Distribution of Delay in Seconds

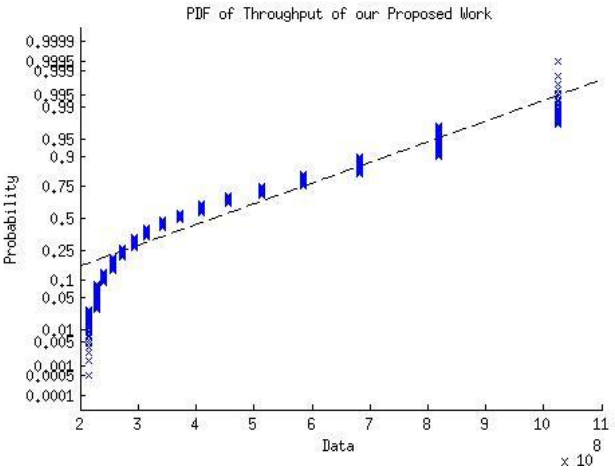

Figure 5: Probability Distribution of Throughput requirements

The graph clearly suggests that very large delays can be seen (suggesting more requests) but not much throughput is required (affected) which is great and showcases the given concept's potential.

V. Conclusion and Future Scope

In this paper, a new hierarchical key management system is presented for MANET based secure communication. Such a distributed key generation and multi-level key generation allows high security and past and future secrecy which is highly needed in applications of MANET as it is being an ad-hoc system and a node can leave of join the network at any time. With this system it can be seen that, the throughput is not affected much even with higher request which is common in large networks. This proves that the given system can be expanded to large networks.

References

[1] Verma, Ekta, Jibi Abraham, and Snehlata Yadav. "Design of Energy Efficient Scheme for Conducting Secure E-Class Application on MANET."Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on. IEEE, 2009.

[2] Dhillon, Danny, et al. "Implementing a fully distributed certificate authority in an OLSR MANET." Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE. Vol. 2. IEEE, 2004.

[3] Boneh, Dan, and Matthew Franklin. "Identity-based encryption from the Weil pairing." SIAM Journal on Computing 32.3 (2003): 586-615.

[4] Umaparvathi, M., and Dharmishtan K. Varughese. "Evaluation of symmetric encryption algorithms for MANETs." Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on. IEEE, 2010.

[5] Matin, Md Abdul, et al. "Performance evaluation of symmetric encryption algorithm in MANET and WLAN." Technical Postgraduates (TECHPOS), 2009 International Conference for. IEEE, 2009.

[6] Jung, Sunsook, Nisar Hundewale, and Alex Zelikovsky. "Energy efficiency of load balancing in MANET routing protocols." Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-Assembling Wireless Networks. SNPD/SAWN 2005. Sixth International Conference on. IEEE, 2005.

[7] Zhang, Qi, and Dharma P. Agrawal. "Dynamic probabilistic broadcasting in MANETs." Journal of parallel and Distributed Computing 65.2 (2005): 220-233.

[8] Eschenauer, Laurent, and Virgil D. Gligor. "A key-management scheme for distributed sensor networks." Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002.

[9] Capkun, Srdjan, Levente Buttya, and Jean-Pierre Hubaux. "Self-organized public-key management for mobile ad hoc networks." Mobile Computing, IEEE Transactions on 2.1 (2003): 52-64.

[10] Du, Wenliang, et al. "A key management scheme for wireless sensor networks using deployment knowledge." INFOCOM 2004. Twenty-third AnnualJoint conference of the IEEE computer and communications societies. Vol. 1. IEEE, 2004.