Journal of Fundamental and Applied Sciences

ISSN 1112-9867

Available online at http://www.jfas.info

Research Article

Special Issue

MANET KEY MANAGEMENT VIA MOBILE FICLKE KEY PROTOCOL (MFK)

S. Shahadan*, K. Farahah, and A. F. A. Firdaus

Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Melaka, Malaysia

Published online: 17 October 2017

ABSTRACT

Mobile Ad Hoc Network (MANET) emerges as one of the popular network as it provides an infrastructure-less protocol to allow mobile devices to send and receive data between one another. However, due to its wireless nature, it is susceptible to various malicious attack such as DoS, wormhole and man-in-the-Middle. As a result, key management protocol has been created in order to overcome this problem. SKiMPy protocol has been designed to send protected data with symmetric shared key in MANET. However, there are several changes need to be done in this protocol predominantly towards improving the delay process of key transmission. Therefore, Mobile Fickle Key (MFK) protocol is proposed to solve the problem. The protocol is tested on an ns-2 simulation environment and it is indicated that MFK performs better than SKiMPy in terms of both time delay and connectivity.

Keywords: MANET; key management scheme; simulation environment.

Author Correspondence, e-mail: shahadan@melaka.uitm.edu.my

doi: http://dx.doi.org/10.4314/jfas.v9i5s.53

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a wireless network that interconnects mobile node without hub, and server [1].The topology of this network is dynamic due to the connectivity of the network may have various way and new node can be added freely during the process of connecting [2]. MANET is known as a platform for emergency situation such that during hurricane or fire where a wired network is not feasible. It can also be used in military operation to transmit sensitive data within a secure connection.

MANET is a self-configured network where all nodes within this network are able to appear and removed freely. This allow it to form a dynamic topology. Each nodes in MANET can act as router or host without any control center. It has bandwidth-constrained and variable capacity link as the node in the network that join with multiple wireless links can be heterogeneous in nature [3]. Devices that utilizes this network are laptop, tablet, PC, and smart phone. This network is therefore susceptible to both internal and external attack due to it lacks of administration center and infrastructure-less nature. Man-in-the-Middle (MITM), Data Traffic, HELLO Flood, Sybil, and session hijacking attack [4]are some of the example attacks in MANET.

Key management in MANET ensures secure transfers of data by decrypting and encrypting a messages using technique such as cryptography. Simple Key Management Protocol (SKiMPy) has been introduced in 2005 by [5] from Department of Informatics, University of Oslo that sets up a symmetric shared key between devices.This protocol utilizes pre-installed certificate to secure the transmission of data third party intervention [6].

The problem that occurs in SKiMPy however is the fact that this protocol requires a time interval in order to select the best key to be shared between nodes in network [5]. For example, keyA, keyB, and KeyC where; (keyA>keyB and keyB>KeyC); therefore, keyA will choose keyC as the best key to be shared and authenticate. This selection process opens up possibility for MITM to interfere and compromise the network. The selection process is exemplified in Fig. 1.

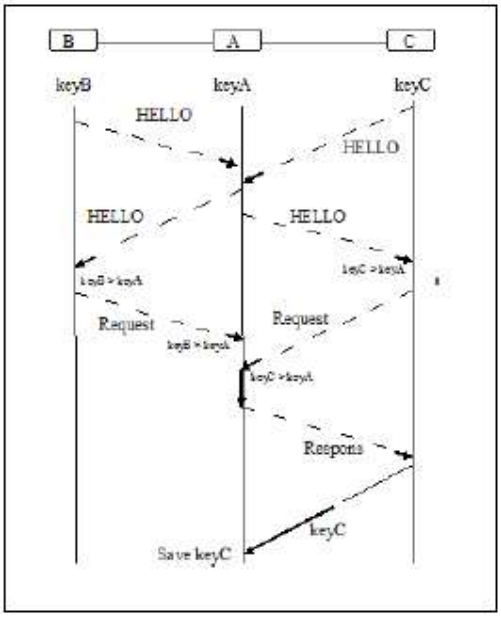

Fig.1. Flow of sharing and key selection

The objective of this project is to design new protocol based on SKiMPy, namely the Mobile Fickle Key (MFK) and compare both protocols to investigate their differences. MFK protocol changes the process of key selection scheme and focus towards sending and receiving data during emergency situation safely in MANET. Furthermore, this protocol is made of two types of messages; Authentication Request (AUTH_REQ) and Authentication Response (AUTH_RESP) to secure the connection of nodes in MANET and prevent malicious attack.

2. MATERIAL AND METHODS

MFK is a key management protocol for MANET in that provides safety and secure network infrastructure between authorized nodes while preventing malicious attacks. This protocol calculates the Receive Signal Strength (RSS) of node to determine the 'strong' and 'weak' node to establish connection to authenticated node. Fig. 2 shows the flow to implement Mobile Fickle Key (MFK).

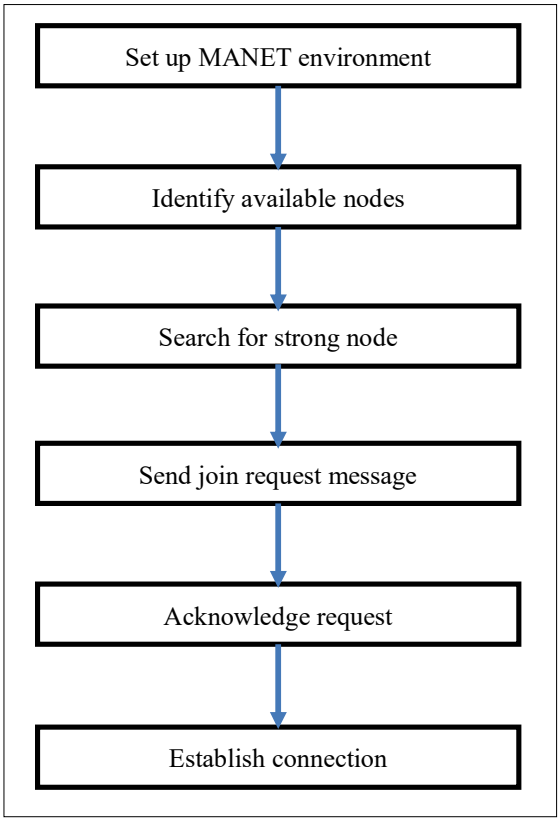

Fig.2.MFK implementation flow

The link quality between each nodesare estimated by ratio of the number from error bits to received bits. This is then updated for every packet receive in certain time. The RSS is calculated based on following formula (1) where α refers to the wavelength of node, Θ refers to the channel gain, and S_{tx} refers to signal power of transmitter (Madhusudhanan, Citra, Rajan, 2015).

$$RSS = \alpha * \Theta * S_{tx} \quad (1)$$

Each nodes measure RSS, mobility and link quality during the exchange of HELLO packet within their neighbors which is stored in Neighbor Table (NT).

Every node has its own power energy, bandwidth and delay that has been set in the script. The following scenario is given as an example: There are three nodes that can be connected, namely Node A (nA), node B (nB) and node C (nC). Node B (nB) is considered as an attacker

(malicious node) while nA and nC serves as the source node and authorized node respectively. First, nA start to search its neighbor as shown in Fig. 3.

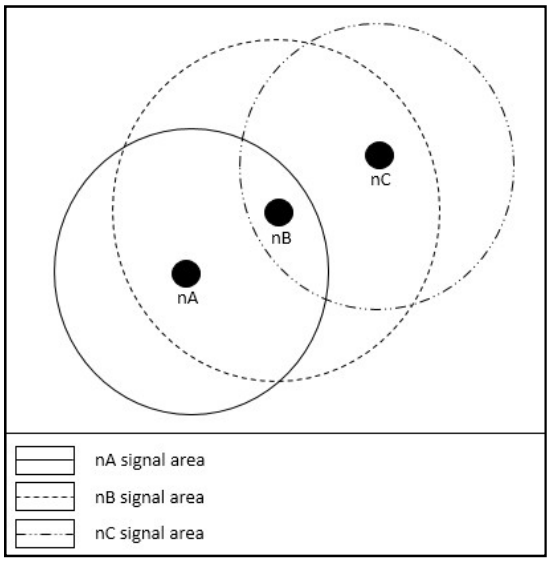

Fig. 3. Nodes signal areas to find neighbor

After determining the strongest and nearest node, nA then sent Authentication Request (AUTH_REQ) to the new node that is nC and nB as shown in Fig. 4.

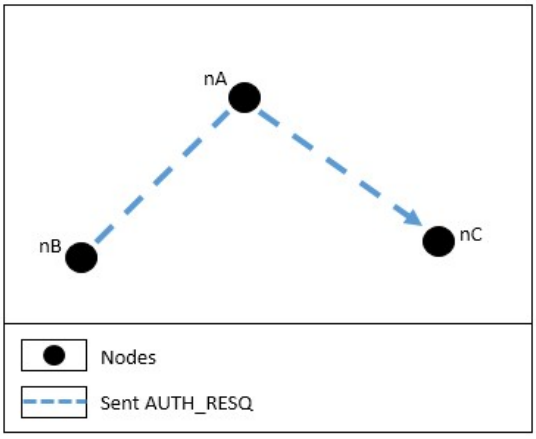

Fig.4. NodeA and B send HELLO message to Node C

Both nodes nC and nB then receives the request and make comparison of signal strength between nodes by exchanging HELLO packet.

$$nA > nC > nB \quad (2)$$

Equation (2) depicts the measurement of RSS; nC detects nA as a strong node and nB is a weak node, implying nB as an attacker.

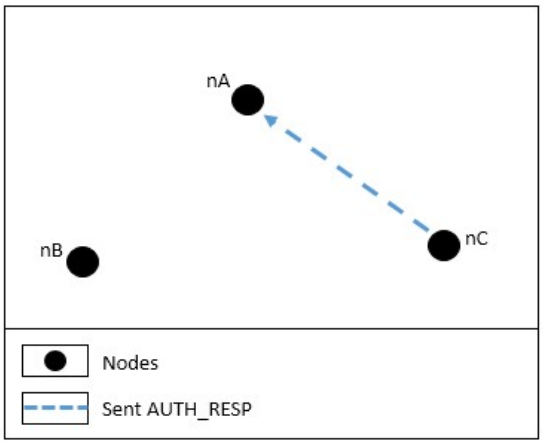

Fig.5. Node C send AUTH_REP to node A

After connection between the nodes are established, nA and nC will exchange their key to send encrypted data in the network securely and safe the connection record to the routing table to be refer in the future use.

3. RESULT AND DISCUSSION

MFK protocol is a key management protocol that is used in MANET to provide safety and secure network infrastructure between authorized nodes and prevent form malicious attack. It calculates the receive signal strength (RSS) of node to determine the 'strong' and 'weak' node so that it can connect to authenticated node. This protocol can secure more in the transmission data for rescue and emergency network such as military, police, fire department and medical center that contain very sensitive data in MANET.

To obtain the comparison between the first implementation of SKiMPy and MFK protocol, a simulation environmenthas been set up for both of the protocol in Network Simulator 2 (ns-2) software with the use of TCL script. To set MANET environment, a specific features need to be added in the script that is shown in Table 1 illustrates the MANET environment features for the simulation:

Table 1.MANET environment features

Channel Type	Channel/Wireless Channel
Radio-Propagation Model	Propagation/Two Ray Ground
Network Interface Type	Physical/Wireless Physical
MAC Type	Queue/Drop Tail/Primary Queue
Link Layer Type	Link Layer
Antenna Model	Antenna/Omni Antenna
Maximum Packet in Queue Length (ifq)	50
Number of Mobile Node	10/20
Routing Protocol	AODV
Time of Simulation End	150

The simulation environment consists of features such as channel type, radio-propagation model, network interface type, MAC type, interface queue type, Link Layer type, antenna model, maximum packet in queue length, number of mobile node used, routing protocol, and time of simulation end. The sizes of the simulation area tested are 500 x 500 and 1000 x 1000 square field while; the number of node tested is 10 and 20 nodes.

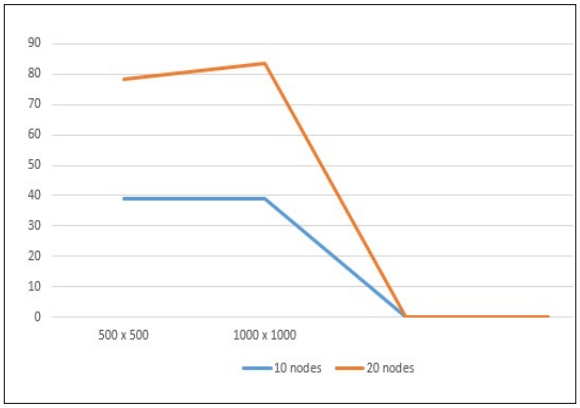

Fig.6.SKiMPy connection speed for 10 and 20 nodes

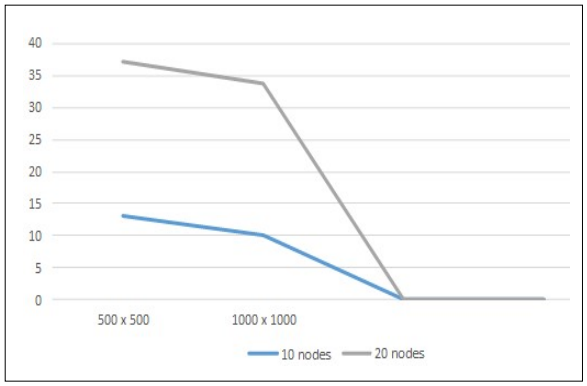

Fig.7.MFK connection speed for 10 and 20 nodes

Based on Fig. 6 and Fig. 7 it is shown that MFK significantly improves the delay time in SKiMPy. In 500x500 paremeter area, MFK protocol took less than 15 seconds to secure the connection among 10 nodes while SKiMPy protocol took almost 40 seconds. In 1000x1000 parameter area, MFK protocol improves the delay time even more by only requiring 10 seconds to detect and establish connections. Similar results are also depicted when simulated using 20 nodes. MFK protocol halves the delay time taken by SKiMPy protocol with less than 40 seconds in 500x500 parameter area. This is also further confirmed by simulation in 1000x1000 area, with MFK further improves the time delay.

The results for securing of the nodes in the network in these two protocol also is shown in Table 2 by comparing both of the key with the valid certificate, detection of attacker node, and time:

Table 2. Difference between SkiMPy and MFK protocol

Features	SKiMPy	MFK
Valid Certificate	Installed by trusted authority	Installed by trusted authority
Detection of attacker node	Determine the time of key (worst key is the attacker node)	Detect using calculation of strength signal
Time Delay	Long time delay	Short time delay

Based on Table 2, both SKiMPy and MFK requires the trusted authority to install the certificate to guarantee that the public and private key is not fully self-organized. In terms of key management to detect and prevent the network from malicious attack, MFK indicates a better performance to detect the attacker due to it use an RSS technique to calculate and prevent the attacker based on the wavelength of node, channel gain and signal power of the node. For the third comparison SKiMPy took considerable time delay to search the entire network for better key than the source node's key compared to the short time delay of MFK.

4. CONCLUSION

In conclusion, MFK has better key management protocol to produce better performance than SKiMPy. The employment of RSS calculation to reduce the delay time occur in previous SKiMPy is shown to be an effective measure. This in turns, allow a faster connection to be established between authorized nodes in MANET. This can be especially beneficial since MANET can be employed in emergency situation [5] which necessitates a reliable and quick connection establishment.

6. REFERENCES

[1]Ohta T, Hashimoto T, andKakudaY. Self-organizing real-time service dissemination and collection using mobile agents for mobile ad hoc networks. In 14th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops, 2011, pp. 199-206

[2] BakshiA.Significance of mobile ad hoc networks. International Journal of Innovative Technology and Exploring Engineering, 2013, 2(4):1-5

[3] Kumar P,Porambage P, Ylianttil M, andGurtovA. A mobile object-based secret key distribution scheme for wireless sensor networks. In IEEE 10th International Conference on Ubiquitous Intelligence & Computing, 2013, 656-661

[4] Bhattacharyya A.Different types of attacks in mobile ADHOC network: Prevention and mitigation techniques. Institute of Engineering & Management, 2011

[5]Pužar M,Andersson J, Plagemann T, andRoudierY. SKiMPy: A simple key management protocol for MANETs in emergency and rescue operations. InR.Molva, G. Tsudik, & D. Westhoff (Eds*)*,Security and privacy in ad-hoc and sensor networks.Heidelberg: Lecture Notes in Computer Science, 2005, pp. 14-26

[6]Madhusudhanan B, Citra S, and RajanC.Mobility based key management technique for multicast security in mobile ad hoc networks. The Scientific World Journal, 2015, 1-10

How to cite this article:
Shahadan S, Farahah K, Firdaus A F A. Manet key management via mobile ficlke key protocol (mfk). J. Fundam. Appl. Sci., 2017, *9(5S), 748-757.*