Towards More Realistic Encryption Systems for Wireless Mobile Ad Hoc Networks

Patience G. Mpofu, Department of Computer Science, University of Limpopo

E-mail: pgmpofu@gmail.com

Abstract- A Mobile Ad Hoc Network (MANET) is a network comprising mobile nodes that combine temporarily to form a network. This network does not make use of the usual network infrastructure for example physical cables and a central facility for management and network administration. How a MANET should be secured is currently an active field of research. However, most methods used to secure MANETs are an adaptation of security measures for conventional wired networks. The security methods arising from these adaptations usually result is security solutions that are inefficient and make assumptions that do not take the unique characteristics of MANETs into consideration. This paper proposes a security solution based on the characteristics, functionalities and goals of these unique networks. We propose a simple encryption system based on the Diffie-Hellman key agreement protocol. The work presented in this paper is intended to shift the direction of research to build security primitives recognized for use by MANETs alone.

Index terms – symmetric keys, MANET security, key management

I. INTRODUCTION

The demand for connectivity between mobile devices for example laptops and handheld devices has led to a shift from conventional static networks to the formation of temporary, infrastructure- less networks. These networks are called Mobile Ad Hoc Networks (MANETs). Difficulty in securing these networks lies in the unique characteristics of these networks. Firstly, they have no central entity for configuring the network, managing keys and performing administrative duties. All nodes within the network perform cooperative functions that ensure the smooth operation of the network. This makes the network robust to node failure. The network has a dynamic topology because nodes may join or leave the network at any time without affecting its operability. Additionally, the nodes are not restricted in movement, they may move to any location at will. All the characteristics of MANETs may be summarized as follows:

- Limited computational power, limited battery power, Limited storage capacity, Dynamic topology, Free movement of nodes, Distributed nature, No central authority for management, No supporting infrastructure, Limited power supply, No prior setting up, Shared transmission medium (air).

Security systems that we design should be able to cater for the above-mentioned characteristics as well as the basic functionalities and goals of a network. These are availability, confidentiality, integrity, non-repudiation, authentication and control of access of information and network assets.

II. LITERATURE SURVEY

Many approaches have been taken in an attempt to secure MANETs. This survey focuses on the notable approaches taken so far. Encryption systems can be categorized as either symmetric or asymmetric. Symmetric systems use a single key to encrypt and decrypt a plain text message. They comprise random nonce and shared key methods. The large pool of pseudo random generators as well as the number of keys shared stresses the limited computational power of the MANET and is not suitable for these networks. Above all, these techniques require a pre-deployment process that is not characteristic of true ad-hoc networking. Asymmetric systems or public key infrastructures are more popular for use in MANETs [2] [4] [5]. However some of the problems used for the algorithms are very hard, to the point of being unsolvable [5]. Asymmetric algorithms take longer than their symmetric counterparts to solve and use up the computational power of the network. An attempt to combat these issues was made in [4]. The problem here is that nodes are required to be within transmission ranges of each other. The system that we propose here has no such requirement. Other techniques include batch verification, which is significantly slower than symmetric algorithms and threshold cryptography which requires a pre-deployment procedure before it can be applied. The rest of this paper is organized as follows: Section III describes the Diffie-Hellman Agreement Protocol on which our solution is based, Section IV describes our proposed solution, Section V gives a simple example, Section VI evaluates the solution and we conclude in Section VII.

III. DIFFIE-HELLMAN AGREEMENT PROTOCOL

Before we discuss the proposed algorithm, we first look at the pioneering work known as the Diffie-Hellman agreement protocol on which our solution is based. The procedure is as follows:

Suppose G is a finite cyclic group with generator G and P,Q are two entities which wish to share keys in order to communicate then

i. P secretly chooses an integer I_p from the interval $(0-|G|-1)$ at random;

ii. Q also chooses an integer, I_Q from the same interval at random;

iii. P computes $(g)I_p \in G$ and sends it to Q;

iv. Q computes $(g)I_q \in G$ and sends it to P;

v. P computes $((g)I_q)I_P$;

vi. Q computes $((g)I_P)I_q$;

vii. Since $((g)I_P)I_q = ((g)I_P)I_q$ it follows that it can be used as a secret key.

IV. PROPOSED SOLUTION

Suppose P wants to establish a secret key with Q. P will choose an integer I_p a base b and a prime number c. P will then calculate the number $N_P = (b)I_P \mod c$. After this calculation, P sends a unicast message to Q containing N_p, c and b.

Each node in this network will have a Key Management Table (KMT) which will have only two columns: the node ID and the shared key. At this point, the shared key column corresponding to Q is empty. Note also that this table will contain shared encryption keys that have been established with other nodes during prior communications. Upon receiving the message from P, Q secretly chooses an integer I_Q and calculates $N_q = (b)I_q \mod c$ and the shared encryption key $K = (N_P)I_Q$ *mod c*. It then enters the value K against node ID for P. Q will then send the value of $(N_P)^I_Q$ to P. When P receives K it then calculates the shared encryption key $K = (N_Q)I_P$ *mod c*. Once this value has been calculated it is entered into the KMT against node Q's ID. At this point, both nodes are able to exchange information safely.

V. EXAMPLE

We will illustrate how the protocol works with a simple example.

i. Node P chooses $Ip = 6$, $b = 5$ and $c = 23$;

ii. P calculates $Np = 5^6 \mod 23 = 8$;

iii. P then sends $c = 23$, $b = 5$ and $N_p = 8$ to Q;

iv. Node Q chooses $I_Q = 4$;

v. Q calculates $N_q = 5^4 \mod 23 = 4$ and sends it to P;

vi. Q calculates $K = 8^4 \mod 23 = 2$;

vii. P calculates $K = 4^6 \mod 23 = 2$;

VI. POSSIBLE WEAKNESSES

The solution we have just described requires the maintenance of a data structure for storing the shared key and the exchange of just two messages. The requirements are kept at a bare minimum to avoid introducing overhead due to the limited resources of the MANET.

However, this solution is susceptible to man-in the-middle attacks and brute force attacks. In a man-in-the-middle attack a malicious node masquerades as a legitimate node. This can be combated using various authorization techniques already in use such as those in [8] and [9]. It would be much more effective though, to create an authorization server based on MANET characteristics, functionalities and goals as emphasized in this paper. This perhaps may also become a direction for future research. In a brute force attack, the attacker exhaustively tries all possible keys that may be used to encrypt or decrypt a message. Attempting to solve this problem is analogous to attempting to solve the *discrete logarithm problem*. The computational power required to successfully attempt such a feat is very high and may prove to be a deterrent to an attacker.

VII. CONCLUSIONS

We hope that this paper will be able to shift the focus of MANET security research. Specifically, we hope that the focus will shift from the adaptation of security frameworks for traditional, wired networks to security frameworks that take the goals, functionalities and the unique characteristics of MANETs into consideration.

VIII. BIOGRAPHY

Patience Gugulethu Mpofu completed her undergraduate degree in 2011 at the University of Limpopo and is currently studying towards an Honors degree at the same institution. Her research interests include cryptography and its applications in MANETs.

REFERENCES

[1]. W. Diffie and M. Hellman, "New Direction Ins in Cryptography," IEEE Transaction on Information Theory, Vol. IT-22, 1976, pp. 644-654.

[2]. C.P.Fleeger and S.L.Fleeger, "Security in Computing", 4th Edition, Foreword by W.H. Ware, pp 81-82.

[3]. J. Chen and J.Wu, "A Survey of Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks".

[4] S.Capkun, J.Hubaux and L.Buttyan, "Mobility Helps Peer-To-Peer Security", *IEEE Transactions on Mobile Computing*, Vol.5, No 1, 2006, pp 43-51 [5] F. Anjum and P. Mouchtaris, "Security for Wireless Ad Hoc Networks", *Published by John Wiley and Sons*, 2007.

[6] M.B.Krishna and M.N.Donja, "Symmetric Key Management and Distribution Techniques in Wireless Ad Hoc Networks", *Proceedings of the International Conference on Computer Intelligence and Communication Systems, 2011.*

[7]. K.Singh, R.S.Yadav and Ranvijay, "A Review Paper on Ad Hoc Network Security", *International Journal of Computer Science and Security*, Vol.1, No.1, pp 52-69.

[8]. E. Ngai, M. Lyu and R. Chin, "An Authentication Service Against Dishonest Users in Mobile Ad Hoc Networks", *Proceedings of the 2004 IEEE Aerospace Conference*, Big Sky Vol. 2, 6-13 March 2004, pp 1275-1285.

[9]. S.Zhu, S. Xu, S. Setia and S. Jajodia, "LHAP: A Lightweight Network Access Protocol for Ad Hoc Networks", *Ad Hoc Networks*, Vol. 4, No. 5, 2006, pp 567-585.