International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014
ISSN 2229-5518

An Efficient Intrusion Detection System for EAACK Scheme in MANETs using DSAB

Uma Maheswari P, Pushpalatha A

ABSTRACT— The movement from wired network to wireless network has been a trend in the past few years. Comparing to other wireless networks MANETs is important one. MANETs contains the collection of mobile nodes or computers with a wireless transmitter and receiver that communicate with each other. MANETs is a self-configurable and has automatic IP configuration features with several independent nodes. Due to this, MANETs are used in applications like military and in natural disasters. Security measures play an important role in all these applications .Hence it is necessary to include intrusion- detection system for MANETs. The existing techniques in finding the malicious nodes in the presence of false misbehavior report using the three parts of EAACK schemes namely ACK, S-ACK, MRA. These are all acknowledgement based schemes. The cryptography used in EAACK schemes are DSA and RSA for authentication process. Due to the network overhead caused by the DSA and RSA we propose a cryptography algorithm called DSAB (Digital signature with Blowfish Algorithm). It takes less number of bits for encryption and verification process.

Keywords— MANETS, ACK, S-ACK, MRA, DSA, RSA, DSAB

1 INTRODUCTION

Mobile Ad hoc Network (MANETs) is a kind of communication network which is different from the traditional wireless network due to its characteristic of no central administration. It is a self-configurable and autonomous network, and consists of several independent nodes. MANETs in recent years not only seen widespread use in domestic and commercial application areas but also becomes the focus of intensive research. Mobile Ad Hoc Networks (MANETs) are wireless networks in which the mobile nodes exchange information without the help of any predefined infrastructure. In such networks also called spontaneous networks, the nodes collaborate to provide the basic network services. Due to their communication type and resources constraint, MANETs are vulnerable to diverse types of attacks and intrusions.

- *Uma Maheswari P is currently pursuing masters degree program in Computer Science and Engineering in Sri Krishna college of Engineering and Technology*
  E-mail: uma.shants@gmail.com
- *Pushpalatha A is currently working as Assistant Professor in Computer Science and Engineering department in Sri Krishna College of Engineering and Technology.*
  E-mail:pushpalathaa@skcet.ac.in

MANETs is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in mission critical applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANETs ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts and medical emergency situations. Due to these unique characteristics, MANETs is becoming more and more widely implemented in the industry. However, considering the fact that MANETs is popular among mission critical applications, network security is of vital importance.

2 EXISTING SYSTEM

The existing system EAACK (Enhanced Adaptive Acknowledgement) consisted of three major parts namely ACK, Secure-ACK (S-ACK), and Misbehavior Report Authentication (MRA). Digital Signature Algorithm (DSA) is incorporated in this EAACK scheme since they are acknowledgement based schemes.[11]

International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014
ISSN 2229-5518

2.1 ACK

ACK (Acknowledgement) is end to end acknowledge scheme to reduce network overhead when there is no misbehavior is discover. In fig. 1, the node S sends a packet (PACK1) to the destination node D. If the intermediate nodes along the route between S and D are cooperative, the node D successfully receives the packet and D needed to send back the acknowledgement packet (ACK1) to the source node, then the transmission from S to D is successful. Else the node S should switch to S-ACK mode to detect the misbehaving nodes in the route.

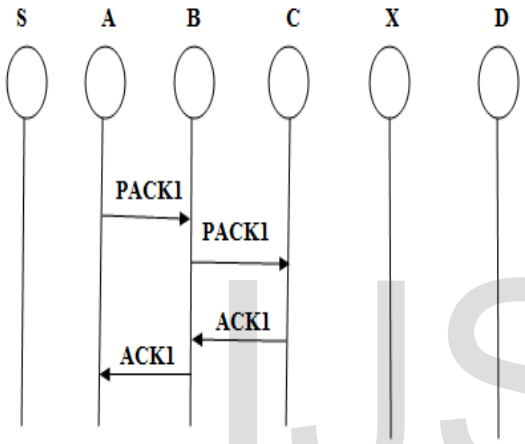

Fig 1. ACK Scheme

2.2 S-ACK

In S-ACK (Secure-ACK) mode the consecutive nodes like E1, E2, E3 work in group to discover the misbehaving nodes in the MANETs network. Node E1 sends out the S-ACK packet to E3 through the intermediate node E2.The node E3 need to send back the S-ACK acknowledgement packet to E1. If the node E1 does not receive the S-ACK acknowledgement packet within the predefined time both E2 and E3 are marked as malicious. The misbehavior report will be generated by the node E1 and send to the source node S. The source node immediately trust the misbehavior report so EAACK need the source node to switch to MRA mode and confirm this misbehavior report.

2.3 MRA

The MRA (Misbehavior Report Authentication) scheme is to authenticate whether the destination node received the reported missing packet through a different route. To start the MRA mode, the source node searches its local base and seeks for an another route to destination route. If no other route exists, the source node starts a DSR routing used to find another alternative path. When the destination node receives the MRA packet, it finds the local knowledge base and compares if the reported packet was received. If the packet is already received then that is the false misbehavior report and who ever created this report is declare as malicious. Else the misbehavior report is trusted and accepted.

2.4 Digital Signature

EAACK is an acknowledgement based IDS. All the parts of EAACK are acknowledgement based schemes. They are based on acknowledgement packets to detect the misbehavior in the MANETS. It is extremely vital to ensure that acknowledgement packets in EAACK are authentic and confidential. If the attackers smart enough to forge acknowledgement packets, these three schemes will be vulnerable. So we incorporated digital signature in our existing system. To bring the integrity of the ID, EAACK requires all packets to be digitally signed before they encrypted and verified. However the extra resources are needed due to the digital signature in the MANETs. To solve this problem in the existing scheme they implemented both RSA and DSA.

3 PROPOSED SYSTEM

3.1 DSAB

To avoid the network overhead caused in existing system by using DSA and RAS , we have introduced another hybrid security by using the Digital Signature and Blowfish Algorithm and compared its performance with the existing algorithms. We have chosen DSA for authentication and Blowfish algorithm for encryption.[14]

3.2 Digital Signature Algorithm

Digital Signature Algorithm (DSA) is based on logarithmic computations and therefore hard to break in. They divide into four categories.[12]

International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014
ISSN 2229-5518

- Global public key component (P, Q, G): P is a prime number where P ranging from 512 < L < 1024 and integer multiple of 64. Q is a prime divisor of (p-1). G is a generator of the subgroup of the order Q mod P such that 1 < G < P.

- Users Private key (X): X is a random integer ranging from 0 < X < Q

- Users Public Key (Y): $Y = G^X \bmod P$

- Users per message secret number (K): K is a random or pseudorandom integer ranging 0 < K < Q

DSA algorithm has two stages. In the first stage, message is signed by the sender. The signature (r, s) along with the message (M) is transmitted to the receiver. The receiver receives the triplet of {M', r', s'}. The second stage occurs at the receiver side by verifying the signature of the message. The functions used in different stages are shown in Table 1.

Table 1. Functions used in DSA

Signing	r= F2(K, p, q, g) = (g k mod p) mod q s= F1(H(M), X, r, q, K) = (K-1 (H(M) + X))mod q Signature= (r, s)
Verification	W = F3(s', q)= $(s')^{-1}$ mod q V = F4(y, p, g, w, r', H(M')) = $[(g^{[h(M')w] \bmod q} y^{(r')w \bmod q}) \bmod p] \bmod q$ Test V= r'

3.3 Blowfish Algorithm

Blowfish a symmetric key block cipher using 64 bits of data blocks and a variable size key maximum up to 448 bits. It included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. The characteristics of Blowfish algorithm is that it includes key dependent S-boxes and has a complex key schedule which makes the algorithm stronger.

3.4 Encryption

The figure.2 shows the action of Blowfish. Each line represents 32 bits. The algorithm keeps two sub key arrays: the 18-entry P-array from(P_1 to P_{18}) and S-boxes. The Function F has four S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XOR with one of the two remaining unused P-entries.

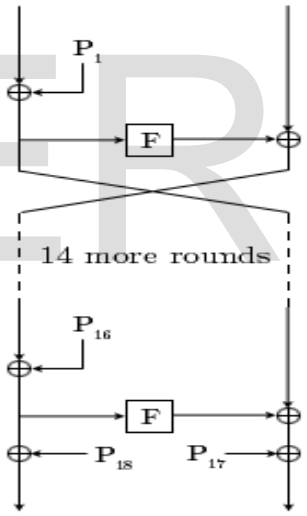

Fig.2 Blowfish Algorithm

The figure.3 shows Blowfish's F-function. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 232 and XOR to produce the final 32-bit output.

International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014
ISSN 2229-5518

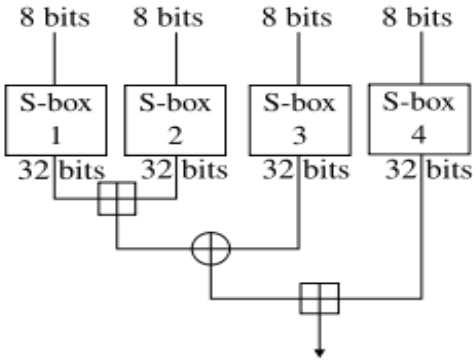

Fig.3 Round function F in Blowfish algorithm

3.5 Decryption

Decryption is exactly the same as encryption, except that P1, P2,…..P18 are used in the reverse order. This is not so obvious because XOR is commutative and associative. A common misconception is to use inverse order of encryption as decryption algorithm (i.e. first XOR P17 and P18 to the cipher text block, then using the P-entries in reverse order)

4 MERGING OF BLOWFISH AND DSA

In wireless network environment messages are transmitted in form of packets. The attacks in the MANETs are due to basically change or modification in data and unauthorized mobile node interception. So it is vital to utilize the both authentication and encryption. The sender encrypts the data packet using the Blowfish algorithm. The encrypted data is then digitally signature by the sender where a random number is generated per message and keep secure or secret. So unauthorized one cannot break through it as the secret number is unknown to the third party. The gain access to the message the third party must need the secret number. So authentication and encryption both are utilized to make the transmission secure enough.

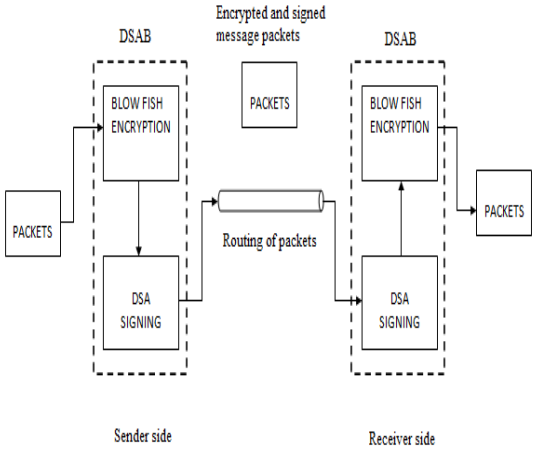

Fig.4 Working of DSA in Routing

5 CONCLUSION AND FUTUREWORK

From the above discussion, we can state that the DSAB approach can avoid network overhead by using limited bits for key generation. And also DSAB is quite efficient to defense the security attacks along with low power consumption. The future work is to eliminate the pre-distributed keys using key exchange mechanism.

6 REFERENCES

[1] G. Jayakumar and G. Gopinath. Ad Hoc Mobile Wireless Networks Routing Protocol – A Review. In Journal of Computer Science 3(8): 574-582, 2007.

[2] B. Sun. Intrusion Detection in Mobile Ad hoc Networks. Doctoral Dissertation. Texas A&M University, 2004.

[3] A. Tabesh, L. G. Frechette, "A Low-Power Stand-Alone Adaptive Circuit for Harvesting Energy From a Piezoelectric Micropower Genera," IEEE Trans. on Industrial Electronics, vol. 57, no. 3, pp. 840-849, March 2010.

[4] Y. Kim, "Remote Sensing and Control of an Irrigation System Using a Distributed Wireless Sensor Network," IEEE Trans. on Instrumentation and Measurement, vol. 57, no. 7, pp. 1379 – 1387, 2008

International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014
ISSN 2229-5518

[5] N. Nasser and Y. Chen. Enhanced Intrusion Detection Systems For Discovering Malicious Nodes in Mobile Ad Hoc Network, In Proceedings of IEEE International Conference On Communication, Glasgow, Scotland, June 24 – 28, 2007.

[6] M. Zapata and N. Asokan. Securing Ad hoc Routing Protocols. In the ACM Workshop on Wireless Security, pp. 1-10, 2002.

[7] K. Kuladinith, A.s Timm-Giel and C. Görg. Mobile Ad-Hoc Communications in AEC industry. In Journal of Information Technology in Construction Vol. 9, pp. 313-323, 2004.

[8] K. Stanoevska-Slabeva and M. Heitmann. Impact of Mobile Ad-Hoc Networks on the Mobile Value System. 2nd Conference on m-Business, Vienna, June 2003.

[9] L. Buttyan and J.P. Hubaux. Security and Cooperation in Wireless Networks. Cambridge University Press, Aug. 2007.

[10] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, J.-B. Viollet, "Which Wireless Technology for Industrial Wireless Sensor Networks? The Development of OCARI Technol," IEEE Trans. on Industrial Electronics, vol. 56, no. 10, pp. 4266-4278, Oct 2009.

[11] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE. EAACK – A Secure Intrusion Detection System for MANETs.

[12] Digital Signature Standard (DSS). Federal Information Processing Standards Publication, National Institute of Standards and Technology, Gaithersburg, MD, 2009 .

[13] R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. In the Communications of ACM, vol. 21, pp. 120-126, 1978.

[14] W. Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .

[15] S. Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," university of Pittsburgh, April 9, 2003. Retrieved October 1,2008.

[16] G. Kumar, M. K. Rai, "An Approach to provide Security in Mobile Ad Hoc Networks using Counter Mode of Encryption on MAC Layer", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

[17]Y. Desmedt and Y. Frankel, "Threshold cryptosystems", in Advances in Cryptology - Crypto '89, Proceedings, Lecture Notes in Computer Science 435, G. Brassard, Ed., Santa Barbara: Springer-Verlag,1990, pp. 307-315.