DSAB – A Hybrid Approach for Providing Security in MANET

Gulshan Kumar[¥], Rahul Saha, Mritunjay Kumar Rai

Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India

¥Corresponding Author: gulshan_acet@yahoo.com

Abstract- With the pace of life, technology has also been evolved. We have moved from the fixed transmission to the mobility aspect. MANETs in todays' environment is of great importance. The dynamic feature of MANETs makes the networks vulnerable to different security attacks. So it is great concern to provide security and authentication along with power utilization and robustness for the MANETs for successful transmission. In our following paper we have introduced our novel hybrid security approach by using digital signature (DSA) with Blowfish algorithm (DSAB) and compared its performance with existing encryption techniques like AES, DES, etc. This article is an extension of the article submitted to ISCTURKEY 2012, Ankara, Turkey.

Keywords- DSAB; DSA; Blowfish; efficiency; energy; encryption.

1. Introduction

In this present era, mobility is a main issue of our life. Day by day the increasing rate of mobile users and other mobile entities creates a great concern on the issue of security.

MANET or Mobile Ad hoc Networks is a unstructured dynamic network comprises of mobile nodes that can join or walk out any time in the network. So, MANET is likely to be vulnerable to the malicious activities of intruders. But with the growth of this kind of network, it is necessary to provide a security mechanism for MANET in such a way which can provide strong authentication property and security [1,3] too along with other constraints like energy-efficient, low-cost, easy implementable, etc. So, we have chosen DSA (digital signature algorithm) for authentication and verification of identity and Blowfish algorithm for encryption purpose.

1.1.Security Attacks in MANET

The present attacks on MANET highly concentrated around DoS. The different types of attacks are listed in Table 1.

Table 1. Attacks in MANET

Layers	Attacks
Application	Repudiation, data corruption
Transport	Flooding
Network	Worm hole, Black hole
Data link	Traffic analysis
Physical	Eavesdropping, Jamming
All	DoS

Repudiation

Non-repudiation refers to the fact of denying transmission of a message or a data packet by either of sender or receiver. It is a kind of passive attack.

Data corruption

Data corruption occurs due to some modification, fabrication operation by the intruders in the transmitted data. Intruders actively take part in this kind of attacks and therefore it is an active attack.

Flooding Attack

The malicious node which is may be or may not be a part of a MANET may send huge number of request packets to a node which is part of the network and thus may disrupt the availability of the service of the victim node. This attack is a form of denial of service attack. Fig.1 represents flooding attack.

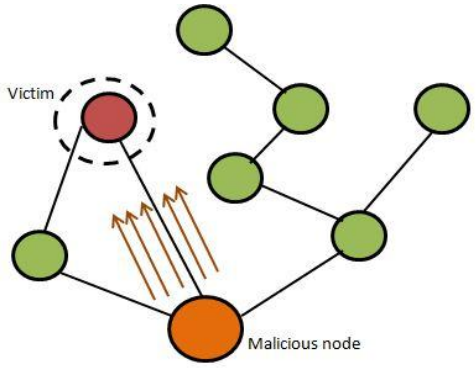

Fig.1. Flooding Attack

Worm hole

In this attack intruders are more than one with a high speed link in use. Requests go through the attacker zone to the destination using the high speed link. Destination confirms this false high speed link as an optimum route and replies back. As a result, all data transmission is open to the malicious nodes. Fig.2 represents a schematic diagram for worm hole attack.

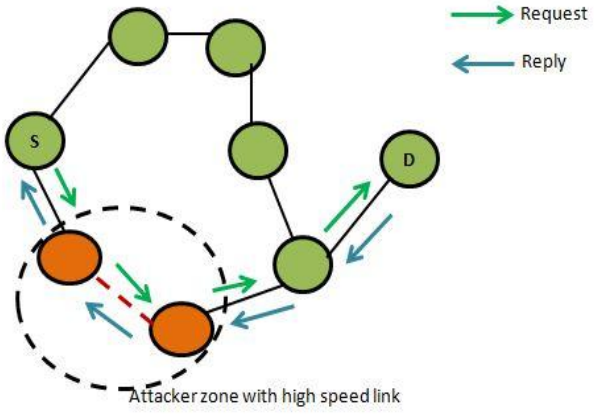

Fig.2. Wormhole attack

Black hole

The entire data pass through the malicious node as it claims itself to be the optimum route by fabricating the sequence number in packets higher than the other nodes and sends fake reply to the source. Fig.3 represents black hole attack.

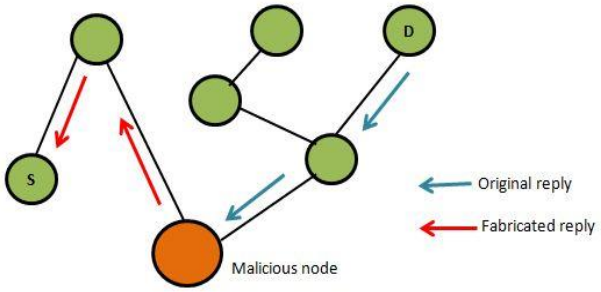

Fig.3. Black hole attack

Traffic analysis

The intruder attempts to guess the traffic being transmitted between the sender and receiver. It is a passive attack which is difficult to detect but easy to defense by implementing required encryption technique. Fig.4 represents traffic analysis scheme.

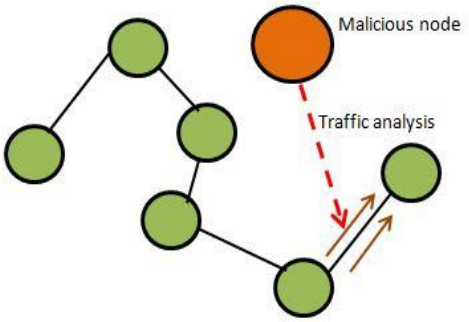

Fig.4. Traffic analysis

Eavesdropping

Eavesdropping attack in MANET shares the wireless medium, as wireless medium make it more vulnerable for MANET malicious nodes to intercept. The attacker node intercepts the transmission as every MANET node is equipped with transceiver in range of the communication which can be decode by means of malicious node to target the authorized node on the network, malicious node can obtain the sensitive information etc. modify the routing route or poison the routing table.

Jamming

Jamming is one of many exploits used compromise the wireless environment like MANET. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. Jamming can result in denial of service attack.

Denial of Service

It is an extended version of jamming attack. It can occur in any layer. Denial of Service refers to the situation where a service is made unavailable to the legitimate users by sending huge number of requests to the service at a time.

1.2. Security Services

Authentication refers to the confirmation and verification of the identity of the communicating parties. Peer-to-peer authentication is confirmed at the establishment or at the run time of a data transmission. Data origin authentication confirms the source identity.

Confidentiality refers to the maintenance of the privacy of the message being transferred from source to destination so that the message content is not revealed to a third party.

Integrity is defined in the term of originality of the message i.e. the message must be transmitted from source to destination without any alteration (in the same way as created and sent by the sender). This security service encounters mostly active attacks.

Non-repudiation deals with storing the proof of data transmission by both sender and the receiver so that neither of them can deny its responsibility later.

Availability ensures the presence of network services despite of security attacks.

2. DSAB (DSA with Blowfish)

From the discussion of the security attacks, we can say that MANET is vulnerable to the malicious activities. Using a strong authentication algorithm along with an encryption technique can overcome the security problems. Therefore, we have chosen DSA (Digital Signature Algorithm) for authentication purpose and Blowfish algorithm for encryption.

2.1. Digital Signature Algorithm (DSA)

Digital Signature Algorithm (DSA) [2] is based on logarithmic computations and therefore hard to break in. The requirements for DSA are classified into four categories.

Global public key component (p, q, g): p is a prime number ranging $2^{L-1} < p < 2^{L}$ where L is the bit length of p ranging from $512 \leq L \leq 1024$ and integer multiple of 64. q is a prime divisor of (p-1) where $2^{159} < q < 2^{160}$. 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 or pseudorandom integer ranging $0 < x < q$.

Users' public key (y): $y = g^{x} \bmod p$

Users' per message secret number (k): k is a random or pseudorandom integer ranging $0 < k < q$.

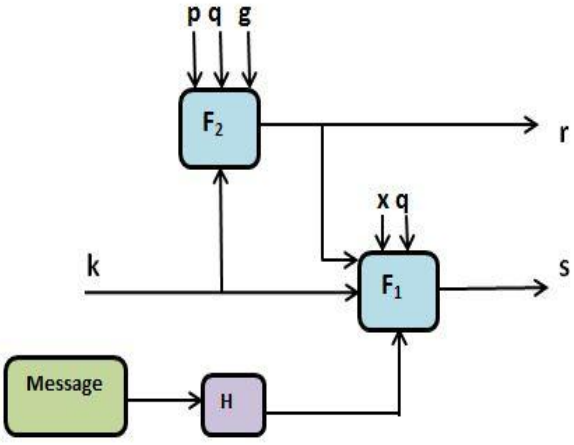

Fig.5. Signing in DSA (sender)

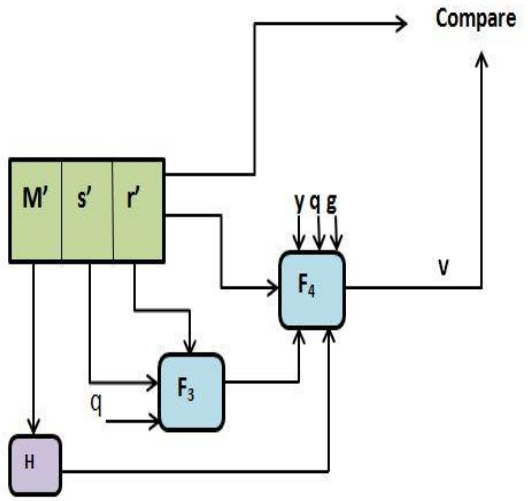

Fig.6. Verification Process (receiver side)

DSA algorithm has two stages. In the first stage, message is signed by the sender. Fig.5 represents the signature process and functions in DSA in sender side. This signature (r, s) along with the message (M) is transmitted to the receiver. The receiver receives a triplet of { M', r', s'} where M', r', s' are the received versions of M, r and s respectively. The second stage occurs at receiver side by verifying the signature of the message shown in Fig.6. The different functions used in different stages are shown in Table 2.

Table 2. Functions used in DSA

Signing	$r = F_2(k, p, q, g) = (g^{k} \bmod p) \bmod q$ $s= F_1(H(M), x, r, q, k) = (k^{-1}(H(M) + xr)) \bmod q$ Signature= (r, s)
Verification	$w = F3(s', q) = (s')^{-1} \bmod q$ $v = F4(y, p, g, w, r', H(M')) = [(g^{[H(M')w] \bmod q} y^{(r')w \bmod q}) \bmod p] \bmod q$ Test v = r'

2.2 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 comprises of Feistel Network having 16 times iterative operations of a simple encryption function. The prime characteristics of Blowfish algorithm is that it includes key dependent S-boxes and has a complex key schedule which makes the algorithm stronger.

Encryption

The data block of 64 bits are first divided into two halves of 32 bits each. Each line in the diagram of the Blowfish algorithm represents 32 bit data. It uses two sub key arrays 18-entry P-array and 256-entry S-boxes. The S-boxes convert the 8 bit input into 32 bits output. One entry of P-array is compulsory for each of 16 rounds as shown in the Fig.7. The remaining two P-array entries are used after the final round to separately XOR the outputs of each of the halves of the data block of 32 bits. In the function F, four S-boxes and two types of bit operations: XOR and addition of modulo 2^{32} are used. The function F first divides the input of 32 bits into four S-boxes of consisting 8 bits each. The outputs of first and second S-boxes are first added to modulo 2^{32} and the output is XOR ed with the third S-box output. The result of XOR operation and the output of fourth S-box is finally added to modulo 2^{32} and we get the final 32 bit output from the function F. The round function operation is shown in Fig.8.

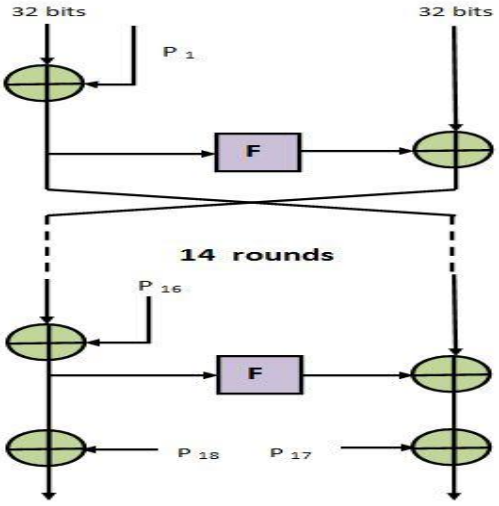

Fig.7. Blowfish Algorithm

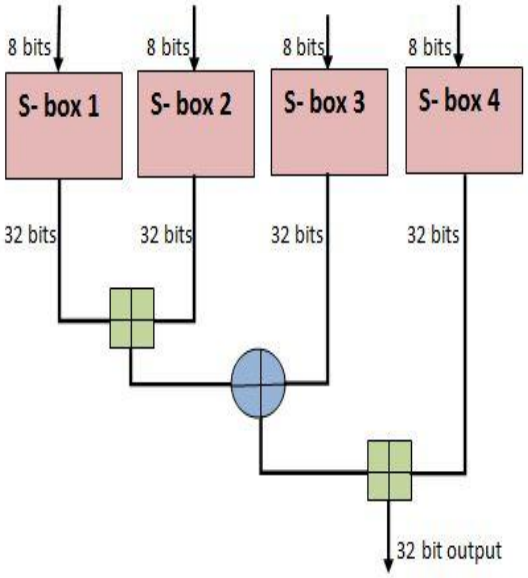

Fig.8. Round function F in Blowfish

The key schedule of Blowfish algorithm starts by initializing the P-array and S-boxes with values derived from the hexadecimal value of pi (∏). The secret key is then byte wise XOR-ed with all the P-entries in order. Many implementations may support 576 bit key size as the P-array is 576 bits long (18 * 32 bits) and the bytes are XOR-ed with all these bits.

Decryption

Decryption is exactly the same as encryption technique except the P1, P2 ……. P18 are used in reverse order.

2.3. Merging of Blowfish and DSA

In wireless network environment messages or data are transmitted in form of packets. The attacks in the MANET environment are due to basically fabrication or modification in data and unauthorized mobile node interception. So, it is needed to utilize the both authentication and encryption. The sender creates a data packet and encrypts with Blowfish Algorithm. The encrypted data is then digitally signature by the sender where a random number is generated per message and keep secret. So, any other third party cannot break through it as the secret number is unknown to the third party. To 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.

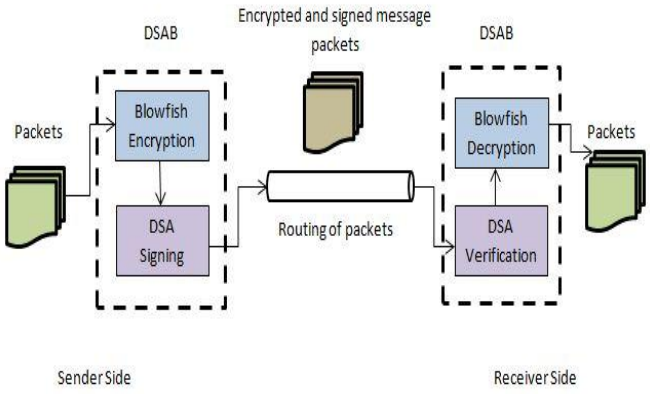

Fig.9. Working of DSAB in Routing

3. Results

For the purpose of simulation we have used NS-2. While simulating we had a network of 100 nodes on 1500 X 1000 area size where the radio range is 200 m and simulation time is 60 seconds considering Constant Bit Rate (CBR). The packet size is considered of 512 bytes. We also considered Taking Random Way Point Mobility Model and varying speed to 10, 20, 30, 40, 50 m/s where Pause time is 5 m/s. We have analyzed the performance of DSAB based on the efficiency in terms of robustness to the attacks, the speed of the algorithm, energy consumption. For this we have considered the packet size of 64 bits, key size of 64 bits and 16 rounds of operation. We have also compared our algorithm with other encryption algorithm like AES and DES. The results are shown below.

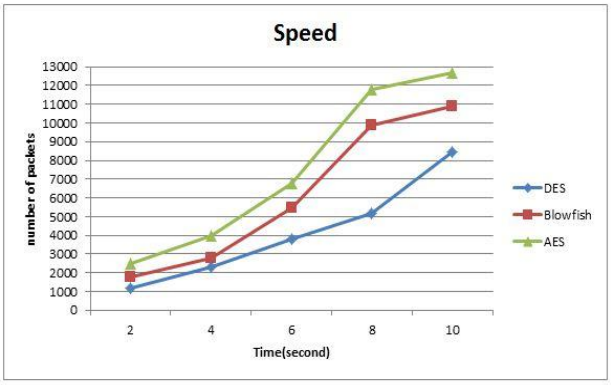

Fig.10. Comparison of symmetric ciphers on speed

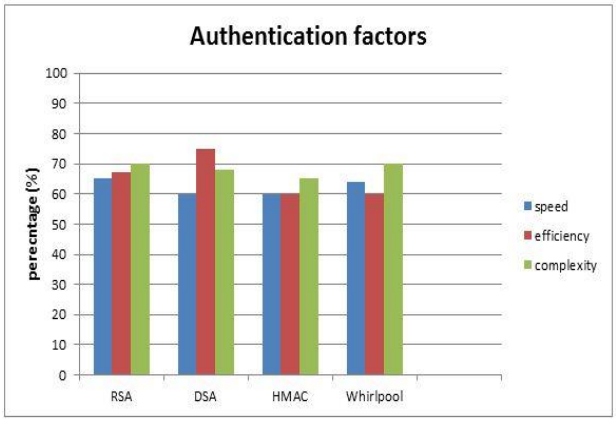

Fig.11. Comparison of authentication protocols

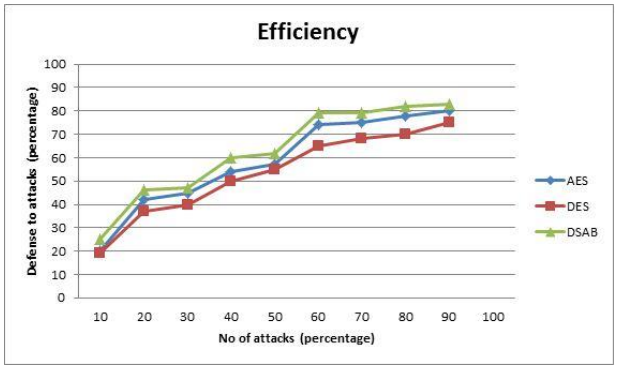

Fig.12. Comparison of DSAB with AES and DES

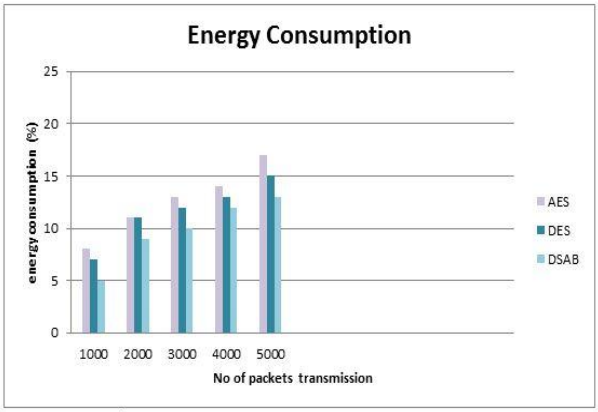

Fig.13. Comparison on energy consumption

According to the statistical analysis of the results found during the experiment and simulation of the work, DSAB is near about 15% more efficient in term of algorithmic speed and cryptologic aspects, than the other approaches compared here. It is also observed that power consumption of DSAB is near about 25% less than AES or DES. Power consumption is measured by the number of dead nodes in a particular time interval in a particular simulation environment. From the above results of our work, we can easily say that our approach of DSAB is quite efficient to defense the security attacks along with low energy consumption.

4. Conclusion

From the above discussion, we can state that our DSAB approach can provide security, confidentiality and authentication. Though the speed of AES is higher than the Blowfish, still we are using it as the energy consumption is low for Blowfish and it can provide same level of security as like AES and with DSA its performance gets better as we have seen above. In future, we would like to work on the complexity levels of the algorithms used here.

References

[1] H.M. Kader and M.M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms," Performance Evaluation, pp. 58-64, 2009.

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

[3] M.N. Islam, M. Mia, M. Chowdhury, M.A.Matin, ”Effect of Security Increment to Symmetric Data Encryption through AES Methodology” Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008 (SNPD '08). 6-8 Aug. 2008, pp.291–294, Phuket, Thailand.

[4] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, “Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks”, In Proceedings of PerCom pp.324-328, 2005.

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

[6] 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.