Implementation of EAACK to Detect Node Misbehavior in MANETs using Intrusion Detection Method

Harshavardhan
P.E.S.I.T.M, Shivamogga

Supriya R K
P.E.S.I.T.M, Shivamogga

Shivanand R D
B.I.E.T, Davanagere

ABSTRACT

Agroup of freely migrating nodes called Mobile Ad hoc NETwork (MANET) is one of the most important and unique wireless network architecture. MANETs do not have fixed infrastructure.Because of its open medium and wide distribution of nodesMANET is vulnerable to malicious attackers. For this reason, it is necessary to design an efficient intrusion detection mechanism to protect MANET from attacks. As it is proposed, that Enhanced Adaptive Acknowledgement (EAACK), a new intrusion detection system can protect MANETs from attacks compared to other IDS approaches due to its special design. EAACK also demonstrates higher malicious behavior detection rates, without affecting the network performances. In this paper we provide an implementation for the above mentioned approach.

Keywords

MANET; Digital Signature, DSA, EAACK

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of autonomous mobile nodes that communicate with each other via wireless link over a range of bandwidth and equipped with both a wireless-transmitter and receiver.

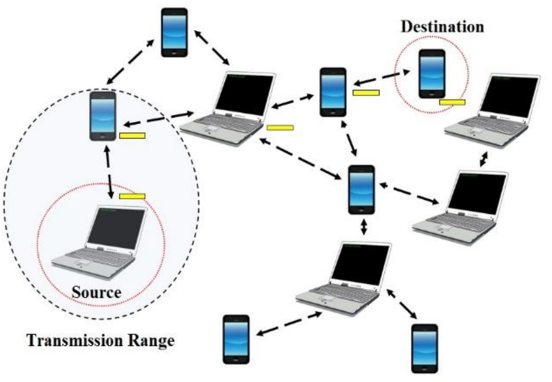


Figure 1: Representation of MANETs

One of the major advantages of wireless networks is its ability to maintain their mobility after the communication of data between different sources. However, the communication is possible in the bandwidth range of transmitters. This means that two nodes cannot communicate with each other when they are beyond the communication range. This problem is solved by MANET by allowingthe intermediate parties to relay data transmissions. For this purpose, MANET is divided into two types of networks, namely, single-hop and multi-hop. In a single-hop network, all nodes that are in the same bandwidth range communicate directly with each other. Whereas, in a multi-hop network, if the destination node is out of its bandwidth range then the nodes will depend on other intermediate nodes to transmit. In contrary to the traditional wireless network, MANET has no fixed network infrastructure. Thus in MANETs, all nodes are free to move randomly. The operation of MANETs does not depend on pre-existing infrastructure or base stations.MANET creates a self-configuring and self-maintaining network without the help of a centralized infrastructure. MANET is often infeasible in mission critical applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET is used in situation where a suitable infrastructure is not availableor is impossible to install.It is mainly used in situations like natural or human-induced disasters, military conflicts and medical emergency situations. Now-a-days MANET is widely implemented in the industry. Since the MANET is widely used in mission critical applications, network security is of vital importance. Compared to wired networks, MANETs arevulnerable to various types of attacks because to the open medium and dynamic node distribution. For example, the malicious attacker can easily capture and compromise nodes to achieve attacks due to the lack of physical protection among nodes'. Most routing protocols in MANETs assume that all nodes in the network cooperatively maintain connectivity with other nodes and assuming that nomalicious attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network.

2. INTRUSION DETECTION SYSTEM IN MANETS

The limitations of most MANET routing protocols is that the nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, Intrusion Detection System (IDS) should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at first time. IDSs usually act as the second layer in MANETs, we mainly describe three existing approaches, namely, Watchdog, TWOACK and AACK.

2.1 Watchdog

The aim of the watchdog scheme is to improve throughput of network with the presence of malicious nodes. In fact, the watchdog scheme is consisted of two parts, namely Watchdog and Path rater. The purpose of Watchdog scheme is that it serves as an intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviors in the network. Watchdog detects malicious misbehaviors by carefully listening to its next hop's transmission. If the next node fails to forward the packet within a certain period of time, watchdog increases its failure counter. Watchdog node reports it as misbehaving if a node’s failure counter exceeds a pre-defined threshold. In this case, to avoid the reported nodes in future transmission, the Path rater cooperates with the routing protocols.

In the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power,4) false misbehavior report, 5) collusion, and6) partial dropping. Watchdog scheme fails to detect malicious misbehaviors.

2.2 Twoack

With respect to the six weaknesses of Watchdog scheme, by acknowledging every data packets transmitted over each three consecutive nodes along the pathfrom the source to the destination, TWOACKdetects the misbehaving links. Upon retrievalof a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing. The receiver collision and limited transmission power problems posed by Watchdog is successfully solved by TWOACK scheme.

2.3 Aack

A new scheme called Adaptive ACKnowledgement (AACK) was proposed based on TWOACK scheme. Similar to TWOACK, AACK is an acknowledgement-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK.

3. DIGITAL SIGNATURE

Digital signature is a mechanism used to protect the integrity of the information.Digital signature is an integral part of cryptography. Cryptography is a practice and techniques for secure communication in the presence of the third parties. In general, cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

The security in MANETs is defined as combination of processes, procedures and systems used to ensure confidentiality, authentication, integrity, availability, and non-repudiation. Digital signature is a widely adopted approach to ensure the authentication, integrity and non-repudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form).

Digital signature schemes can be mainly divided into the following two categories:

1. Digital Signature: In the signature verification algorithm, the original message is required. Example: Digital Signature Algorithm (DSA).

2. Digital Signature with Message Recovery: This type of scheme requires the signature itself in the verification process and no other information is required.

The general flow of data communication with digital signature is as shown in fig2.

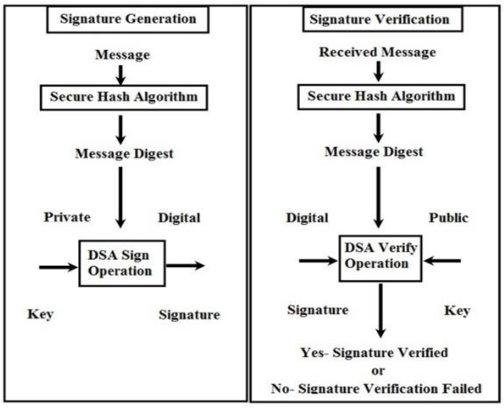


Figure 2: Communication with digital signature

4. PROBLEM DEFINITION

The proposed approach [1] in EAACK can help to avoid three of the weaknesses of Watchdog method. They are: false misbehavior, limited transmission power and receiver collision. Here we implement these three weaknesses. EAACK mainly constituted of three major parts. They are: ACKnowledge (ACK), Secure-ACKnowledge (S-ACK) and Misbehavior Report Authentication (MRA).

4.1 ACK

ACK is an end-to-endacknowledgement method. It is the basic approach in EAACK, for reducing network overhead in times where there are no misbehavior in network.

4.2 S-Ack

S-ACK method is similar to TWOACK with some added security. Here as proposed, each three consecutive nodes will work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node. The introduction of S-ACK is mainly to find the misbehaving in the presence of receiver collision or limited transmission power.

4.3 MRA

The Misbehavior Report Authentication (MRA) method is implemented to solve some of the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. False misbehavior report could be generated by malicious attackers that report few of the regular working nodes as malicious, which is a false report and must be corrected. This kind of report can be misleading and can damage to the entire network thus cause a network division by breaking down the sufficient nodes required for transmission. The center of MRA approach is to check whether the destination node has received the reported missing packet through a different route.

To start with MRA mode, the source node will first search its local knowledge base and seek for alternative route to the destination node. If there are no other route exists, then source node will start a DSR routing request to find new route to destination node. Because of this nature of MANETs, it is common to find multiple routes between any two nodes.

5. IMPLEMENTATION

The EAACK scheme is implemented by using the algorithms like DSA and RSA with the introduction of Digital signature with RSA is used to prevent the attackers from forging acknowledgement packet. The EAACK scheme requires all the acknowledgement packets to be digitally signed before they are sent out and verified until they are accepted and extra resources are required with the introduction of digital signature in MANETS, the security of DSA is high and more efficient.

5.1 Digital Signature Algorithm

Digital signatures are essential is used to verify the sender of a document's identity. A digital signature is represented in a computer as a string of binary digits.The signature is computer using a set of rules and parameters (algorithm) such thatthe identity of theperson signing the document as well as theoriginality of the data can be verified. The signature is generated by the use of a private key. A private key is known only to the user. The signature is verified makes use of a public key which corresponds to the private key. With every user having a public/private key pair, this is an example of public-key cryptography. Public keys, which are known by everyone, can be used to verify the signature of a user. The private key, which is never shared, is used in signature generation, which can only be done by the user.

The DSA algorithm procedure can be explained as.

5.1.1 DSA Key Generation

The DSA key generation steps are as follows

Step 1: Firstly shared global public key values (p, q, g) are chosen:
Step 2: Choose a large prime p=2L
    Where L=512 to 1024 bits and is a multiple of 64.
Step 3: Choose q,a 160 bit prime factor of p-1
Step 4: Choose g=h(p-1)/q
    For any h<p-1, h(p-1)/q(mod p)>1
Step 5: Each user chooses a private key and computes their public key:
    Choose x<q,compute y=gx(mod p)

5.1.2 DSA Signature Creation and Verification

The DSA signature creation and verification steps are as follows

Step 1: To sign a message M
    Generate random signature key k,k<q compute

- $R=(g^k(\text{mod } p))(\text{mod } q)$
- $S=k^{-1}SHA(M)+x.r(\text{mod } q)$

Send signature (r,s) with message.

Step 2: To verify a signature,compute

- $w= s^{-1}(\text{mod } q)$
- u1=(SHA(M).w)(mod q)
- u2=r.w(mod q)
- v=(gu1.yu2(mod p))(mod q)

if v=r then the signature is verified.

5.2 RSA Algorithm

The RSA Algorithm (named after its inventors Rivest, Shamir and Adleman) is a widely used for public key cryptography.

Based on exponentiation in a finite (Galois) field over integers modulo aprime number. Exponentiation takes O((log n)3) operations.Uses large integers (eg. 1024 bits).Security due to cost of factoring large numbers nb. Factorization takes O (e log n log log n) operations.

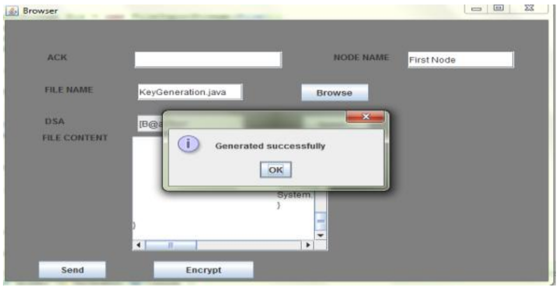
The RSA algorithm steps are as follows.

Step 1: Each user generates a public/private key pair by selecting two large primes at randomp,q
Step 2: Computing their system modulus N=p.q
    Where z(N)=(p-1)(q-1)
Step 3: Selecting at random the encryption key e
    Where1<e<z(N), gcd(e,z(N))=1
Step 4: Solve following equation to find decryption key d
    e.d=1 modz(N) and 0<=d<=N
Step 5: Publish their public encryption key: KU={e,N}
    Keep secret private decryption key: KR={d,p, and q}
Step 6: To encrypt a message M the sender:
    -obtains public key of recipient KU={e,N}
    -Computes: C+Me mod N, where0<=M<N
Step 7: To decrypt the ciper text c:
    -uses their private key KR={d,p,q}
    -computes: M=Cd mod N

6. EXPERIMENTS AND RESULTS

This chapter deals the results of the EAACK scheme with the use of key properties of DSA with RSA and explains the results with the help of snapshots as shown in proceeding steps.

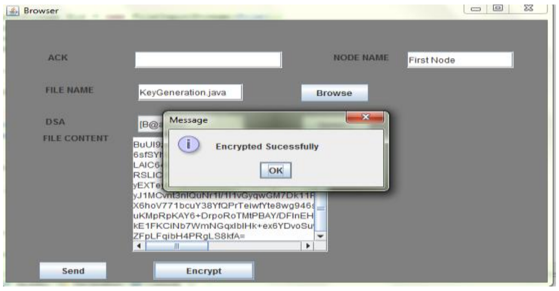
6.1 Results



ACK
NODE NAME First Node
FILE NAME KeyGeneration.java
DSA [B@
FILE CONTENT
Generated successfully

Figure 3: Source node generates dsa key

In the above fig 3 states that the source node generates the dsa with rsa key while sending the data to intermediate node.



Browser

ACK

NODE NAME: First Node

FILE NAME: KeyGeneration.java

DSA: [B@a

FILE CONTENT:

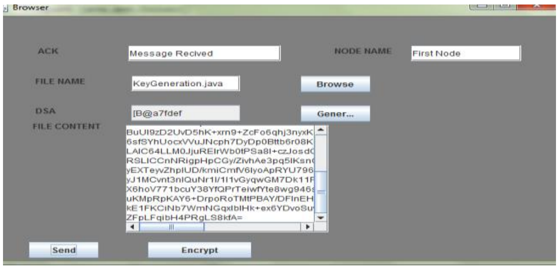
BuUI9z
6sfSYh
LAIC6
RSLIC
yEXTe
yJ1MCvnt3nIQuNr1I/1I1vGyqwGM7Dk11F
X6hoV771bcuY38YfQPrTeiwfYte8wg946s
uKMpRpKAY6+DrpoRoTMtPBAY/DFInEH
kE1FKCiNb7WmNGqxIbIHk+ex6YDvoSu
ZFpLFqibH4PRgLS8kfA=

Message

Encrypted Sucessfully

Figure 4: Source node encrypt the data

In the fig 4 states that after generating the keys the source node encrypt the data and send the data to destination.



Browser

ACK: Message Recived

NODE NAME: First Node

FILE NAME: KeyGeneration.java

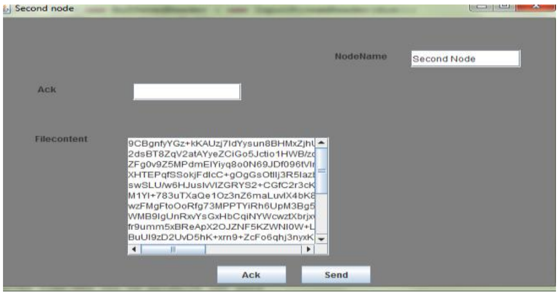
DSA: [B@a7fdef

FILE CONTENT:

BuUI9zD2UvD5hK+xrn9+ZcFo6qhj3nyxK
6sfSYhUocxVVuJNcph7DyDp0Bttb6r08K
LAIC64LLM0JjuREIrWb0tPSa8I+czJosd0
RSLICCnNRigpHpCGy/ZivhAe3pq5IKsn
yEXTeyvZhpIUD/kmiCmfV6IyoApRYU796
yJ1MCvnt3nIQuNr1I/1I1vGyqwGM7Dk11F
X6hoV771bcuY38YfQPrTeiwfYte8wg946s
uKMpRpKAY6+DrpoRoTMtPBAY/DFInEH
kE1FKCiNb7WmNGqxIbIHk+ex6YDvoSu
ZFpLFqibH4PRgLS8kfA=

Figure 4: Sending the data to the intermediate node

In the fig 4 states that the source node encrypts the data and the message is sent successfully to the destination through intermediate node.



Second node

NodeName: Second Node

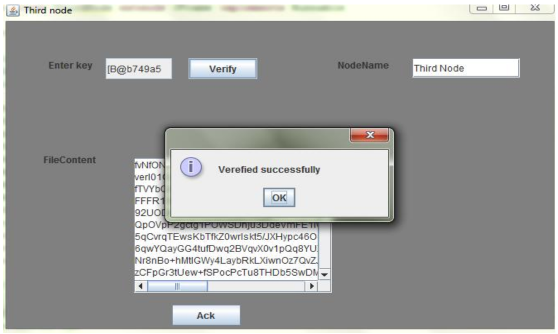
Ack

Filecontent:

9CBgnfyYGz+kKAUzj7IdYysun8BHMxZjhU
2dsBT8ZqV2atAYyeZCiGo5Jctio1HWB/zc
ZFg0v9Z5MPdmEIYiyq8o0N69JDf096tVIr
XHTEPqfSSokjFdIcC+gOgGsOtIIj3R5Iazt
swSLU/w6HJusIvVIZGRYS2+CGfC2r3cK
M1YI+783uTXaQe1Oz3nZ6maLuvIX4bK8
wzFMgFtoOoRfg73MPPTYiRh6UpM3Bg5
WMB9IgUnRxvYsGxHbCqiNYWcwztXbrjx
fr9umm5xBReApX2OJZNF5KZWNI0W+L
BuUI9zD2UvD5hK+xrn9+ZcFo6qhj3nyxK

Figure 5: The intermediate node contains data

In the fig 5, the intermediate node receives the file contents from the source node and this data sent to the destination node.



Third node

Enter key: [B@b749a5

NodeName: Third Node

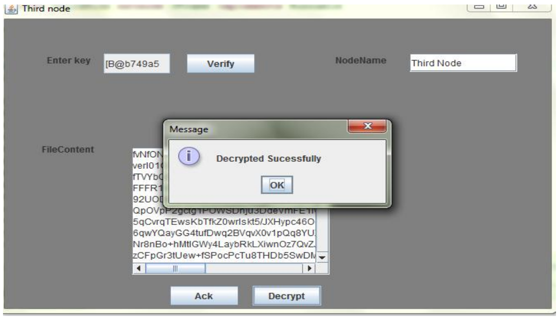
FileContent:

fvNfON
verl01
fTVYb
FFFR1
92UOD
QpOVpF2gctg1POWSDnju3DdevmFE1
5qCvrqTEwsKbTfkZ0wrlskt5/JXHypc46O
6qwYQayGG4tufDwq2BVqvX0v1pQq8YU
Nr8nBo+hMtIGWy4LaybRkLXiwnOz7QvZ
zCFpGr3tUew+fSPocPcTu8THDb5SwDM

Verefied successfully

Figure 6: Destination node verifies the key

In the fig 6 states that destination node receives the data from source that contents of the data to be verified through the dsa key.



Third node

Enter key: [B@b749a5

NodeName: Third Node

FileContent:

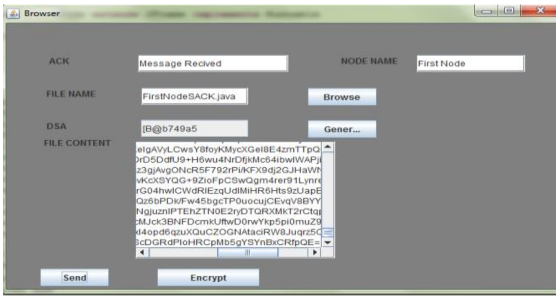
fvNfON
verl01
fTVYb
FFFR1
92UOD
QpOVpF2gctg1POWSDnju3DdevmFE1
5qCvrqTEwsKbTfkZ0wrlskt5/JXHypc46O
6qwYQayGG4tufDwq2BVqvX0v1pQq8YU
Nr8nBo+hMtIGWy4LaybRkLXiwnOz7QvZ
zCFpGr3tUew+fSPocPcTu8THDb5SwDM

Message

Decrypted Sucessfully

Figure 7: Destination node decrypts the data

In the fig 7 shows that the destination node receives the data from source and decrypts the contents of the data by using the dsa and rsa keys and send back the acknowledgment to the source node.



Browser

ACK: Message Recived

NODE NAME: First Node

FILE NAME: FirstNodeSACK.java

DSA: [B@b749a5

FILE CONTENT:

eIgAVyLCwsY8foyKMycXGeI8E4zmTTpQ
rD5DdfU9+H6wu4NrDfjkMc64ibwIWAPj
z3gjAvgONcR5F792rPi/KFX9dj2GJHaWN
vKcXSYQG+9ZIoFpCSwQgm4rer91Lynre
rG04hwICWdRIEzqUdIMiHR6Hts9zUapE
Qz6bPDk/Fw45bgcTP0uocujCEvqV8BYY
NgjuznIPTEhZTN0E2ryDTQRXMkT2rCtq
MJck3BNFDcmkUftwD0rwYkp5pi0muZ9
kI4opd6qzuXQuCZOGNAtaciRW8Juqrz5C
cDGRdPIoHRCpMb5gYSYnBxCRfpQE=

Figure 8: Source node receives Ack from destination

In the fig 8 states that source node receives the Ack from destination without fail of any data.

7. CONCLUSION AND FUTURE WORK

Mobile Ad-hoc network is the active research area that is being wide spread due to lot of application in military and civilian communication. This kind of network asks for cooperation of all its members in networking function, which makes it vulnerable to attacks. This intern affects the routing. The misbehaving nodes participating in network Route Discovery phase can cause severe degradation as per performance of the network as they refuse to forward the data packets.

In this paper, we studied some of the problems faced in terms of security forMANETs. Also we have implemented the proposed approach called EAACK, which is specifically designed for MANETs. The evaluation of its performance with respect to existing system such as watchdog, TWOACK andAACK shows drastic improvement and overcomes its weaknesses like receivercollision, limited transmission power and false misbehavior report.

To increase the merits of the research work, we are planning to investigate the following issues in our future research:

1. Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature.

2. Examine the possibilities of adopting key exchange mechanism to eliminate the requirement of pre-distributed keys.

3. Testing the performance of EAACK in real network environment instead of software simulation.

8. REFERENCES

[1] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE "EAACK—A Secure Intrusion-DetectionSystem for MANETs", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

[2] R. Akbani, T. Korkmaz and G.V.S Raju. "Mobile Ad hoc Network Security", Lecture Notes in Electrical Engineering, vol. 127, pp. 659-666, Springer, 2012 – here1

[3] R.H. Akbani, S. Patel, D.C. Jinwala. "DoS Attacks in Mobile Ad Hoc Networks: A Survey", the proceedings of the Second International Meeting of Advanced Computing & Communication Technologies (ACCT) , pp. 535-541, Rohtak, Haryana, India. 2012. – here1

[4] Y. Hu, D. Johnson and A. Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In the Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, pp. 3-13, 2002.

[5] 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.

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

[7] 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.