International Journal of Science Engineering and Advance Technology

Acknowledgement based Intrusion-Detection System for MANETS

[1.]D.Gayathri, [2.]Dr.M.S.S.Sai
[1] M Tech Student, [2]Professor
[1,2]Dept of Computer Science and Engineering,
[1,2]KKR & KSR Institute of Technology & Sciences ,Vinjanampadu, Guntur Dt,A.P.

Abstract

In the next generation of wireless communication systems, there will be a need for the quick deployment of independent mobile users. notable examples include establishing survivable, efficient, flush communication for emergency/ recover operations, defeat relief efforts, and Army networks. Such network scenarios cannot count on centralized and organized connectivity, and can be make up as applications of Mobile Ad Hoc Networks. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. The self configuring ability of nodes in MANET made it popular among critical mission applications like army use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is decisive to develop efficient intrusion-detection mechanisms to protect MANET from attacks. By using technology support we are cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security problem. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially made for MANETs. Compared to contemporary approaches, Enhanced Adaptive ACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

Index Terms: Digital signature, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgment (AACK) (EAACK), Mobile Ad hoc Networks (MANET).

1. Introduction

Due to their natural mobility and scalability, wireless networks are always preferable since the first day of their invention. Owing to the improved technology and reduced costs, wireless networks have gained much more preferences over wired networks in the past few decades.

1.1 What is MANET:

In the next generation of wireless communication systems, there will be a need for the quick deployment of independent mobile users. Notable examples include establishing survivable, efficient, flush communication for emergency/ recover operations, defeat relief efforts, and Army networks. Such network scenarios cannot count on centralized and organized connectivity, and can be make up as applications of Mobile Ad Hoc Networks. [2]. MANET is actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Or else, a stand for Mobile Ad Hoc Network [18]. A MANET[29] is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi [17][19] connection, or another medium, such as a cellular or satellite transmission.

To divide data D into n pieces in such a way that D is easily reconstruct able from any k pieces, but even complete knowledge of k - 1 pieces reveals absolutely no information about D[1].

1.2 Benefits:

Having discussed the general issues in MANETs[11] the behind their popularity and their benefits will now be discussed.

(a) Low cost for deployment: As the name suggests, ad-hoc networks can be deployed on the fly, thus demanding no expensive infrastructure such as copper wires, data cables, etc.

(b) Fast deployment: When conceded to Wirless adhoc networks, ad hoc networks are very convenient purpose and easy to deplorer queering less manual intervention since there are no cables involved.

(c) Flush Configuration: Ad hoc network configuration can change dynamically with time. For the a lot of scenarios such as data sharing in classrooms, etc., this is a needful feature. When compared to configuration of LANs, it is very easy to change the network topology.

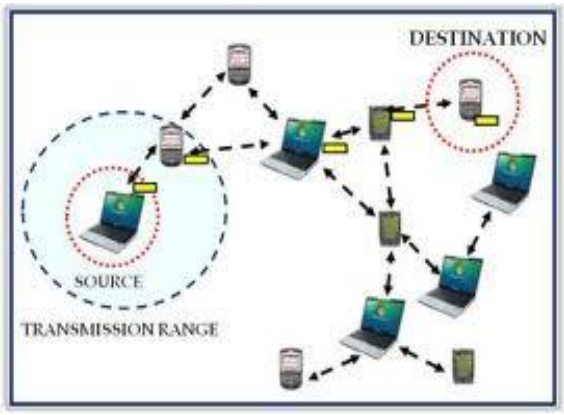

Figure 1.1: Structure of MANET

1.3 How MANET works?

The purpose of the MANET [17] working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and flush topologies with increased flushes due to node motion and other factors.

Approaches are intended to be relatively lightweight in nature, suitable for multiple hardware and wireless environments, and address scenarios where MANET[20] are deployed at the edges of an IP infrastructure. Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers) should also be supported by MANET [18] specification Using mature components from previous work on experimental reactive and proactive protocols, the WG [20] will develop two Standards track routing protocol specifications:

- Reactive MANET Protocol(RMP)
- ProactiveMANETProtocol(PMP)

If significant commonality between RMRP [16] and PMRP [16] protocol modules is observed, the WG may decide to go with a converged approach. Both IPv4 and IPv6 [14] will be supported. Routing security requirements and issues will also be addressed [6]. The MANET [20] WG will also develop a scoped forwarding protocol that can efficiently flood data packets to all participating MANET nodes.The primary purpose of this mechanism is a simplified forwarding function. The usage of this protocol is intended to be applied ONLY within MANET routing areas and the WG effort will be limited to routing layer design issues. The MANET WG will pay attention to the OSPF-MANET protocol work within the OSPF WG and IRTF work that is addressing new research topics related to MANET environments.

2. System Analysis

2.1 Existing System:

By definition, Mobile Ad hoc Network (MANET) [11] is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. inadequately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' absence of physical protection [5], malicious attackers can easily capture and compromise nodes to achieve attacks.

In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily adjustment MANETs by inserting malicious or non cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology [11], a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is pivotal to develop an intrusion-detection system (IDS) specially designed for MANETs.

Disadvantages Of Existing System:

Watchdog(wd) scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; 6) partial dropping.

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog(wd). However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overflow. Due to the limited battery power nature of MANETs, such unneeded transmission process can easily degrade the life span of the entire network. The concept of adopting a hybrid scheme in AACK greatly reduces the network overflow, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

2.2 Proposed System:

In fact, a lot of of the existing IDSs in MANETs adopt an acknowledgment-based scheme, and adding TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets.

Hence, it is pivotal to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we take on a digital signature in our proposed working scheme named Enhanced AACK (EAACK).

Advantages Of Proposed System:

Our new approach EAACK is designed to tackle three of the six weaknesses of Watchdog(wd) scheme, namely, false misbehavior, limited transmission power, and receiver collision.

3. System Requirement

Specification Modules

Implementation is the stage of the project when the theoretical design is turned out into our working system. Thus it can be considered to be the most critical

stage in achieving a successful our current working system and in giving the user, confidence that the our current working systemwill work and be effective.
The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Modules:

- ACK implementation
- Secure Acknowledgment (S-ACK)
- Misbehavior Report Authentication (MRA)
- Digital Signature Validation

MODULES DESCRIPTION:

ACK implementation:

ACK is basically an end – to – end acknowledgment scheme .It is a part of EAACK scheme aiming to reduce the network overflow when no network misconduct is detected.
The basic flow is if Node A sends an packet p1 to destination Node D, if all the intermediate node are cooperative and successfully receives the request in the Node D. It will send an ACK to the source (Node A), if ACK from the destination get delayed then it S-ACK process will be initialized.

Secure Acknowledgment (S-ACK):

In the S-ACK principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

Misbehavior Report Authentication (MRA):

The MRA scheme is designed to resolve the weakness of wd with respect to the false misconduct report. In this source node checks the alternate route to reach destination. Using the generated path if the packet reaches the destination then it is concluded as the false report.

Digital Signature Validation:

In all the three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all count on acknowledgment packets to detect misconducts in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

4. System Implimentation

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful our current working systemand in giving the user, confidence that the our current working systemwill work and be effective.
The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.
Implementation is the process of converting a our current working systemdesign into operation. It is the phase that focuses on user training, site preparation and file change for installing a candidate system. The important factor that should be considered here is that the change should not disrupt the functioning of the organization.
The implementation can be preceded through Socket in java but it will be considered as one to all communication .For proactive broadcasting we need flush linking. So java will be more suitable for platform independence and networking concepts.

4.1methodology And Algorithm Used:

Enhanced adaptive acknowledgement (EAACK) is an acknowledgement based intrusion detection system; in order to ensure all acknowledgement packets is authentic. They use digital signature algorithm (DSA) to sign the acknowledgement packets digital signature algorithm (DSA) involves more routing overflow and energy consumption, Adopting hybrid cryptography techniques [2]. To further reduce the network overflow caused by digital Signature without compromising its security [6]. This paper proposes Elliptic curve Digital signature algorithm instead of Digital Signature Algorithm to ensure that all acknowledgment packets in EAACK are authentic and untainted. ECDSA stands for "Elliptic Curve Digital Signature Algorithm", it's used to create a digital signature of data (a file for example) in order to allow you to verify its authenticity without compromising its security[6]. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which uses elliptical curve cryptography. Elliptical curve cryptography is considered on an equation of the form: $y^2 = (x^3 + a * x + b) \bmod p$. To sign a message, the curve parameters (CURVE, G, n) must be agreed upon. In addition to the field and equation of the curve, Need G ,a base point of prime order on the curve; n is the multiplicative order of the point G.A private key integer dA, randomly selected in the interval (1,n-1); and a public key curve point QA=dA * G.

4.2 Algoritham Implementaion And Results:

Elliptic Curve Digital Signature Algorithm is implemented over elliptic curve P-192 as mandated by ANSI X9.62 in C language. The Project contains necessary modules for domain parameters generation, key generation, signature generation, and signature verification over the elliptic curve. ECDSA has three phases, key generation, signature generation, and signature verification.

INPUT: ECDSA Key Generation:

An entity A's key pair is associated with a particular set of EC domain parameters D= (q, FR, a, b, G, n, h). E is an

elliptic curve defined over Fq , and P is a point of prime order n in E(Fq), q is a prime. Each entity A does the following:

1. Select a random integer d in the interval [1, n- 1].
2. Compute Q = dP.
3. A's public key is Q, A's private key is d.

ECDSA Signature Generation:

To sign a message m, an entity A with domain parameters D= (q,FR, a, b, G, n, h) does the following:

1. Select a random or pseudorandom integer k in the interval [1,n-1].
2. Compute kP =x1, y1 and r= x1 mod n (where x1 is regarded as an integer between 0 and q-1). If r= 0 then go back to step 1.
3. Compute k-1mod n.
4. Compute s= k-1{h (m)+ dr} mod n, where h is the Secure Hash Algorithm (SHA-1). If s = 0, then go back to step 1.
5. The signature for the message m is the pair of integers (r, s).

ECDSA Signature Verification:

To verify A's signature (r, s) on m, B obtains an authenticated copy of A's domain parameters D = (q, FR, a, b, G, n, h) and public key Q and do the following:

1. Verify that r and s are integers in the interval [1, n-1].
2. Compute w = s-1mod n and h (m)
3. Compute u1 = h(m)w mod n and u2 = rw mod n.
4. Compute u1P + u2Q =(x0, y0) and v= x0 mod n.
5. Accept the signature if and only if v = r

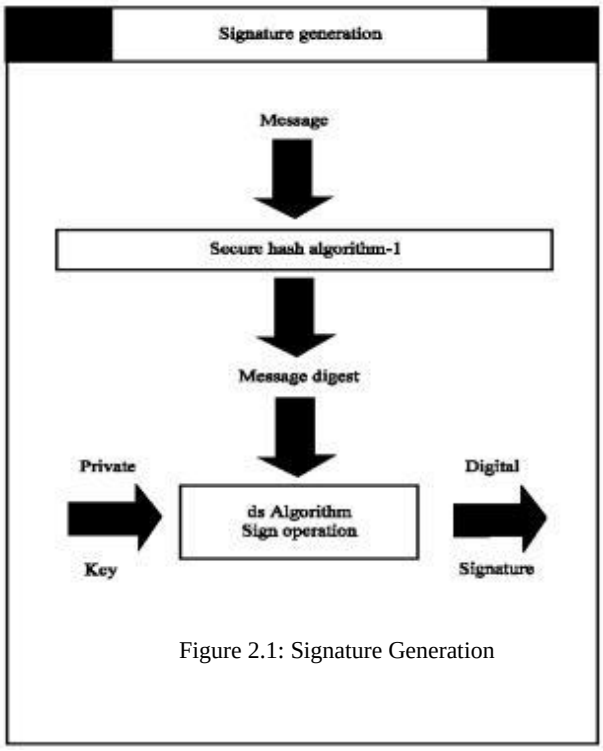

Figure 2.1: Signature Generation

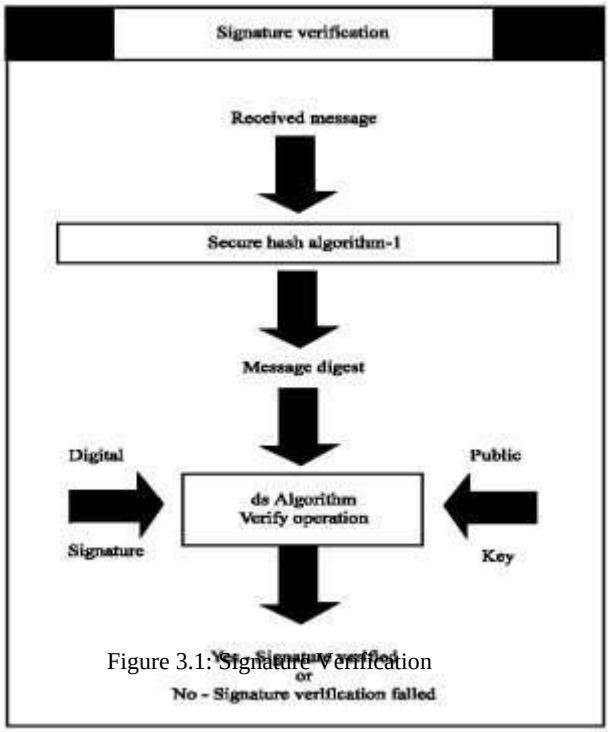

Figure 3.1: Signature Verification

RESULTS

The following results are brought to highlight for given set of values.

The SHA-1 result are shown along with the private and public set of keys

SHA–1
Input: "a"
SHA
Output: 86f7e437faa5a7fce15d1ddcb9eaeaea37667b8
Input: "ABC"
SHA
Output: 3c01bdbb26f358bab27f267924aa2c903fcfdb8

Key Pair Generation:

198 bit random private key and corresponding public key:
Private A= 341070834395747541371049654904959 138812316708511486831983984 65
Public x of A= 308918222585090190199331 01 51334356 466906901301271156815371
Public y of A=293 4312592567055080539 1 06109573501 917061922980571738132 54
Private A= 97847545072694784411473994093 87459926 335654578030561509614891
Public x of A=579435003913255651467015999189 7 674340 9250716115312636030
Public y of A= 100902462247736483225741599 1 97414 564739299641922223243 91

Further for a given input file containing text had been taken and signature is generated and then verified by the values of r and s.

Signature Generation:
Input file="abcd"

Private:0xd43fb7ff56a7486859d87f85db45b043129f6468ccff42d0001
Signature:
r=0xb8d06fa44816c92b8b26f797ef3cc07984d8b7f7e49a33
s=0xd74f17a1e19139d77558c6b216dcb1f4bb31da2dd2573

Proof of verification:

If a signature (r, s) on a message m was indeed generated by A,
then s = k -1 (h (m)+dr) mod n. Rearranging gives k ≡ s-1 (e+dr) ≡s-1e + s-1 rd ≡we +wrd ≡ u1+ u2d (mod n).
Thus u1G +u2Q = (u1 +u2d) G = kG and so v=r as required.

Normally data transmission in MANETs consumes the most battery power. Hence Elliptic curve Digital signature algorithm requires less computational power than Digital Signature Algorithm. Proposed working scheme always produces slightly less network overflow than DSA does. Shorter keys are as strong as long key for DSA, Low on CPU consumption and memory usage.From the results, we conclude that acknowledgment-based schemes, including TWOACK, AACK, and EAACK, are able to detect misconducts with the presence of receiver collision and limited transmission power.we provide the malicious nodes the ability to forge acknowledgment packets. In this way, malicious nodes simply drop all the packets that they receive and send back forged positive acknowledgment packets to its previous node whenever necessary. This is a usual method for attackers to degrade network performance.

5. Conclusion

In this new research paper, we have proposed working a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Wd, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misconduct report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our new research to incorporate digital signature in our proposed working scheme.

We note that for all misconducts, because SACKs are advisory thus allowing a data receiver to renege on all SACKed out-of-order data, eventually the data sender-receiver will timeout, discard all SACK information, and return to a correct state. Thus the data flow remains reliable; only perform ance degradation may occur. As stated in the Introduction, we discovered SACK misconducts during our investigation of data rene ging [7]. In that investigation, we argue that SACKs should be "permanent" (not advisory) meaning a data receiver MUST NOT renege on out-of-order data. If SACKs were to become permanent, since misconduct G can result in unreliable data transfer, it would have to be fixed. While we hope misconducts A-F will be fixed, even if left as is, they will only result in reduced performance, not unreliable protocol behavior. While simple in concept, SACK handling is complex to implement.

6. Future Enhancements

This paper can be investigated the following issues in the future research:

- Possibilities of adopting hybrid cryptography techniquesto further trim the network overflow caused by digitalsignature;
- Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of redistributedkeys;
- Testing the performance of EAACK in real network environmentinstead of software simulation.

7. Acknowledgments

The authors thank Jonathan Leighton, Aasheesh Kolli and Ersin Ozkan for their valuable di scussions and comments while developing this paper. The authors also sincecount thank the anonymous reviewers for their constructive feedback.

8. References

[1] A.Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. National Computer Conf.*, 1979, vol. 48, pp. 313–317.
[3] M.Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT' 94*, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.
[4] M. Naor and B. Pinkas, "Visual authentication and identification," in *Proc. CRYPTO'97*, 1997, vol. 1294, pp. 322–336, Springer-Verlag LNCS.
[5] T. H. Chen and D. S. Tsai, "Owner-customer right protection mechanism using a watermarking scheme and a watermarking protocol," *Pattern Recognit.*, vol. 39, pp. 1530–1541, 2006.
[6] P. Tuyls, T. Kevenaar, G. J. Schrijen, T. Staring, and M. Van Dijk, "Security displays enabling secure communications," in *Proc. First Int. Conf. Pervasive Computing, Boppard Germany, Springer-Verlag Berlin LNCS*, 2004, vol. 2802, pp. 271–284.
[7] C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," *Designs, Codes and Cryptography*, vol. 24, pp. 255–278, 2001.
[8] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Computat.*, vol. 129, pp. 86–106, 1996.
[9] N. K. Prakash and S. Govindaraju, "Visual secret sharing schemes for color images using halftoning," in *Proc. Int. Conf. Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, 2007, vol. 3, pp. 174–178.
[10] H. Luo, F.X.Yu, J. S. Pan, and Z. M. Lu, "Robust and progressive color image visual secret sharing cooperated with data hiding," in *Proc. 2008 Eighth Int. Conf.*

Intelligent Systems Design and Applications, 2008, vol. 3, pp. 431–436.
[11} J. Broch, D. A. Maltz, D. B. Johnson, Y. Hu, J. Jetcheva, A Performance Comparison of Multi-Hop Wireless Ad Hoc network Routing Protocols, Proc. Of MobiCom'98, Oct. 1998
[12]] E. R. Royer, C.-K. Toh, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, , IEEE Personal Communications, Apr. 1999
[13] V. D. Park and M. S. Corson, A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks, , IEEE INFOCOM'97, 1997
[14] Prof. Ravindra Rathod, Prof M. D. Ingle , Prof. Bharat S Kankate , Prof R. M. Kawale
[15] Dr.J.Subash Chandra Bose , U.Akila Devi 2, M.Prasanalaxmi 3 , K.Malathi 4 , K.P.Vinodhini 5 , S.Saranya 6 Professor and Head, Department of Computer Science Engineering, Professional Group of Institutions, Palladam,
[16] K. Fall, S. Floyd, "Simulation-based comparisons of Tahoe,Reno, and SACK TCP", CM Computer Communication Review, 26(3), 6/96, pp. 5-2
[17] K. Fall, S. Floyd, "Simulati on-based comparisons of Tahoe, Reno, and SACK TCP", ACM Computer Communication Review, 26(3), 6/96, pp. 5-2
[18] K.Liu,J.Deng,P.K.Varshney, And K.Balakrishnan -"An acknowledgement-based approach for the detection of routing misbehavior in MANETs".[May-2007]
[19] S . Marti , T . J. Giuli , K . Lai ,and M . Baker, - "Mitigating routing misbehavior in mobile ad hoc networks".[Mar-2000]
[20] T . Sheltami , A . Al-Roubaiey , E . Shakshuki ,and A . Mahmoud,- "Video transmission enhancement in presence of misbehaving nodes in MANETs".[Oct-2009]