Journal of Computer Science

Original Research Paper

Security in MANET's by Using Detective Signature Techniques

Gayathri, A. and P. Narayanasamy

Department of Information Science and Technology, Anna University, Chennai-25, Tamilnadu, India

Article history
Received: 20-06-2014
Revised: 04-09-2014
Accepted: 24-01-2015

Corresponding Author:
Gayathri, A.
Department of Information
Science and Technology,
Anna University, Chennai-25,
Tamilnadu, India
Email: replygayathri@gmail.com

Abstract: Mobile Ad-hoc Network (MANET) is one among the fastest growing area in the field of research where security is a vital factor for protecting MANET against attacks, EAACK is an acknowledgement based IDS which is composed of three parts namely, ACK, S-ACK and MRA along with digital signature to provide security against attacks. Till now contemporary technique such as EAACK with watchdog technique are deployed to detect and avoid intruders whereas this technique does not avoid all intruders because it relies on acknowledgement checking and supervisory node. Hence we propose strong and secure cryptographic technique with the help of combining EAACK with dynamic digital signature using TwoFish Cryptographic Algorithm to overcome the mentioned limitations, in order to authenticate and avoid intruders from communication. In this process NS2 is used to simulate and evaluate the proposed scheme.

Keywords: Digital Signature, Enhanced Adaptive Acknowledgement (EAACK), Mobile Ad hoc Network (MANET), Security, WATCHDOG and NS2

Introduction

Mobile Ad Hoc Networks is a collection of wireless computer in which communication happens among themselves over possible multi-hop paths without fixed infrastructure, namely base stations or access points. Nodes in mobile ad hoc network perform operations by forwarding packets between each other to allow nodes to communicate beyond direct wireless transmission range, there by all nodes in MANET's act as both host and routers. Due to lack of centralized administration or fixed network infrastructure, it can be easily set up without cost when required. Application in MANET includes Military operations, emergent operations, civilian applications like ad-hoc meeting or an ad-hoc classroom, disaster reliefs and electronic device networking are few to mention. The typical types of attacks in MANET's include eavesdropping, address spoofing, forged packets and Denial Of Service (DOS).

Most of the routing protocols in MANET are subject to different type of attack due to lack of fixed infrastructure and dynamic topology. Most of the network in MANET assumes that every node in the network behaves trusty with other nodes and presumably not malicious or non cooperative nodes in the network. In such scenarios, it is crucial to develop an Intrusion-Detection System (IDS) specially designed for MANET's. Many researchers had worked for this topic ever since it's existence (Shakshuki *et al*., 2013).

The remainder of this study is organized as follows. In section II, We present the essential information required for understanding the research topic. In section III, we present problem definition. In section IV, TWOFISH ALGORITHM and working methodology. In section V, the simulation results concerning the performance of the proposed scheme are provided. Section VI, presents the conclusion and future research scopes.

Background of IDS

IDS in MANET's

As discussed earlier, mobile wireless ad hoc networks have different methodologies to overcome the problems of attacks. There are contemporary challenges related to security issues that need to be addressed. Many intrusion detection systems have been proposed and most of them are tightly related to routing protocols (Zhang *et al*., 2003), such as Watchdog/Pathrater (Shakshuki *et al*., 2013) and Route guard. Depending on the detection techniques used (Zhang *et al*., 2003), IDS can be categorized into three types, namely: (1) Signature or misuse based IDS, (2) Anomaly based IDS, (3) Specification based IDS, it is an hybrid of both the signature and the anomaly based IDS.

Signature-Based IDS

Uses pre-known attack scenarios (or signatures) and compare them with incoming packet traffic. There are several approaches in the signature detection, which they differ in representation and matching algorithm employed to detect the intrusion patterns. Some of the detection processes are expert system, pattern recognition, colors petri nets and state transition analysis (Shakshuki *et al*., 2013).

Anomaly-Based IDS

It attempts to detectactivities that differ from the regular expected system behaviour. This detection has severaltechniques name to few, neural networks, statistical analysis, etcand other techniques such as data mining and Chi-squaretest utilization.

Specification-Based IDS

It monitors the current behaviour of systems according to specifications that describe desired functionality for security-critical entities. Any mismatch found between current behaviour and the specifications is termed as an attack.

Existing Work

Watchdog

This method was proposed by Marti *et al.* (2000), the basic idea of the Watch dog mechanism is to police (Called Watch dogs) their downstream neighbours locally using overheard messages in order to detect misbehaviour. The watchdog's work is to detect disobedient nodes by listening to nodes in promiscuous mode. When a node forwards a packet, the watchdog mechanism of that node monitors the subsequent node to confirm that it also forwards the packet correctly. It keeps sent packets in a buffer till the packets are actually forwarded by the respective nodes, then they are removed from the buffer subsequently. If the packets remain in the buffer longer than some timeout period, the watchdog increments the failure count of the node implicated.

When the failure count of a node exceeds a threshold, the node is identified as a misbehaving node and a notification is sent to the source node (Marti *et al*., 2000). It is stated that watchdog can also detect replay attacks to some extent. However, since it uses promiscuous listening, it is stated that it might not detect misbehaving nodes in the existence of ambiguous collisions or receiver collisions; nodes that organize their transmission power to deceive a listener into believing a message has actually been sent and nodes that falsely report other nodes as misbehaving. It cannot detect partial dropping attacks and collaborative attacks involving at least two consecutive malicious nodes in a route. Pathrater finds the most trustworthy path by using link trustworthiness data and misbehaving nodes information from the watchdog (Marti *et al*., 2000). In DSR, there can be many paths from source to destination, but the shortest path is selected.

By using pathrater, the most reliable path is selected as a substitute of the shortest path in the presence of misbehaving nodes. The SRR (send extra route request) extension to DSR can be added to find new paths when all paths include misbehaving nodes (Johnson *et al*., 1996). Pathrater gives ratings to each node and provides a path metric based on the ratings of the nodes on the path. The authors state that ratings of the nodes should be rearranged to prevent permanently excluding temporary misbehaving nodes from routing and forwarding.

If a watchdog detects that a packet is not forwarded within a certain period or is forwarded but altered by its neighbour, it states that neighbour node is misbehaving. When the misbehaviour rate for a node surpasses certain threshold, the source is notified and subsequent packets are forwarded along the routes that exclude the nodes. Watchdog consists of two parts mainly, watchdog and pathrater. Watchdog plays a vital role in detecting malicious nodes rather than other method for Intrusion Detection System (IDS) (Zhang *et al*., 2003), many IDS's are based or developed from the watchdog method (Sheltami *et al*., 2009). The watchdog schemes fails to detect malicious misbehaviours with the presence of following: (1) Ambiguous collisions, (2) receiver collisions, (3) limited transmission power (4) false misbehaviour report (5) collusion and (6) partial dropping.

TWOACK

This method was proposed by (Liu *et al*., 2007). In this TWOACK method; it solves the weakness of WATCHDOG problem, namely receiver collision and limited transmission power problem (Shakshuki *et al*., 2013). Perhaps, the acknowledgment process required in each packet transmission process added a significant amount of unwanted network overhead. There exists, limited battery power nature of MANET's, such as redundant transmission process which can easily degrade the life span of the entire network. Moreover, the research studies are working in energy harvesting to deal with this problem. The working process of TWOACK is shown in Fig. 1. Node 'A' first sends Packet 1 to node B and then node B sends Packet 1 to node C. When node C receives Packet 1,as node A is two hops behind, thennode C will agree to generate TWOACK packet, which containsreverse routefrom node Ato node C and send it back to node A. The TWOACK packet at node A indicates the transmission of packet 1 from node A to node C is successful, If not, TWOACK packet is notreceived in a predefined time period,both nodes B and C are reported as malicious.

This process is repeated forthree consecutivenodes along the rest of the route.

AACK

This method was proposed by (Sheltami *et al*., 2009), It is similar to TWOACK. Basically AACK is a combination of TACK (identical to TWOACK) and end-to-end acknowledgment scheme. AACK is used to reduce the network overhead. Perhaps TWOACK and AACK have the problem to detect malicious nodes with the presence of false misbehaviour report. In order to provide authentication for the acknowledgment packets, there exists digital signature (DS) techniques (Bhalaji, 2008; Rivest *et al*., 1978).

Digital Signature

Digital signature plays a vital role for authentication in security for MANET's (Rivest *et al*., 1978). Digital signature consists of three algorithms, namely:

- A key generation algorithm selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key
- A signing algorithm that, given a message and a private key, produces a signature
- A signature verifying algorithm that, given a message, public key anda signature, either accepts or rejects the message's claim to authenticity

Proposed Problem Definition

The problem definition is framed on the basis to solve the existing issues in WATCHDOG and to overcome from it using techniques which reduces network overhead and thereby attaining better performance.

TWOFISH ALGORITHM

In cryptography, Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish. Twofish's distinctive features are the use of pre-computed key-dependents and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes). Twofish borrows some elements from other designs; for example, the Pseudo-Hadamard Transform (PHT) from the SAFER family of ciphers.

Twofish has a Feistel structure like DES. On most software platforms Twofish has slightly slower than Rijndae l (the chosen algorithm for Advanced Encryption Standard) for 128-bit keys, but it is somewhat faster for 256-bit keys. Twofish was designed by Bruce schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall and Niels Ferguson; the "extended Twofish team" who met to perform further cryptanalysis of Twofish and other AES contest entrants included Stefan Lucks, TadayoshiKohno and Mike Stay.The Twofish cipher has not been patented and the reference implementation has been placed in the public domain. As a result, the TWOFISH ALGORITHM is free for anyone to use without any restrictions whatsoever. It is one of a few ciphers included in the Open PGP standard (RFC 4880). However, Twofish has seen less widespread usage than Blowfish, which has been available longer.

Necessity of Using TWOFISH ALGORITHM

- SIMPLICITY: All the design elements of the algorithm have a clear reason or function
- PERFORMANCE: They compared all the different option on the basis of relative performance
- CONSERVATIVENESS: They left a margin for error and they provided more security than required while trying to design against attacks that are yet known
- CLOCK CYCLE: Encrypt data in less than 500 clock cycle per block on an Intel Pentium, Pentium Pro and Pentium II for a fully optimized version of the algorithm
- KEY: Be capable of setting up a 128-bit key for optimal encryption speed in less than the time required to encrypt 32 blocks on a Pentium Pro and Pentium II. Accept only key length up to 256 bits

Block Diagram for TWOFISH ALGORITHM

The Fig. 2 gives the overview of TWOFISH ALGORITHM from the reference (Yang, 2011).

Working Principle of Proposed Method

Figure 1 the main idea behind this study is to enhance the performance and to avoid malicious node inside the network activity by introducing an Enhanced Intrusion detection technique to overcome the problem of EAACK. EAACK solves the unsolved issues of WATCH DOG (Shakshuki *et al*., 2013). EAACK is the combination of three methods namely ACK, S-ACK and MRA. With this method the dynamic digital signature concept was added to show the avoidance of malicious nodes inside the routing activity using DSA digital signature approach. Our proposed method will work along with TWOFISH ALGORITHM. Enhanced EAACK is a combination of EAACK, dynamic digital signature and TWOFISH ALGORITHM. In our technique, we use strong cryptographic dynamic mechanism called TWOFISH ALGORITHM, where ituses dynamic drastically changing digital signatures which does not repeat again.

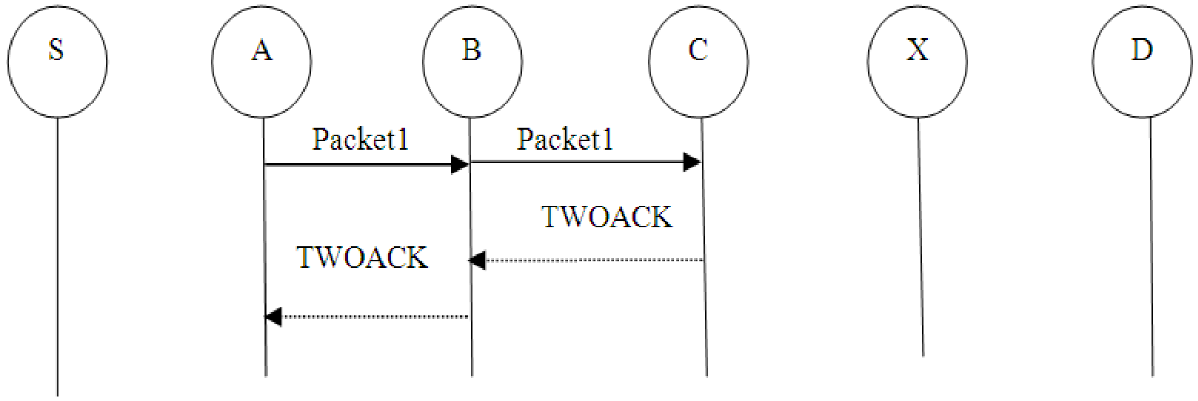

Fig. 1. TWOACK Scheme: In this scheme, each node sends involves in transmission and sends an acknowledgement packet to the node that is two hops away from it

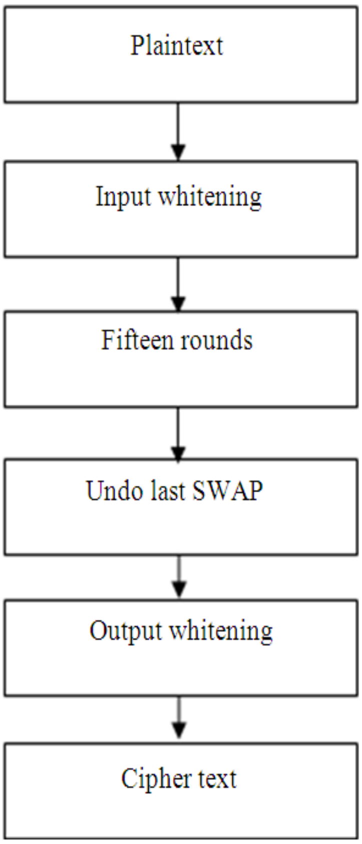

Fig. 2. TWOFISH ALGORITHM

Using this signature, the algorithm converts a message into strong cryptographic segments. These messages are divided and transferred to destination one by one. This makes our technique and safeguards our data's from any sort of attackers (especially all types of DOS attacks). For each nano, milli seconds the signature was dynamically changed for every communication. So that attacks can be overridden.

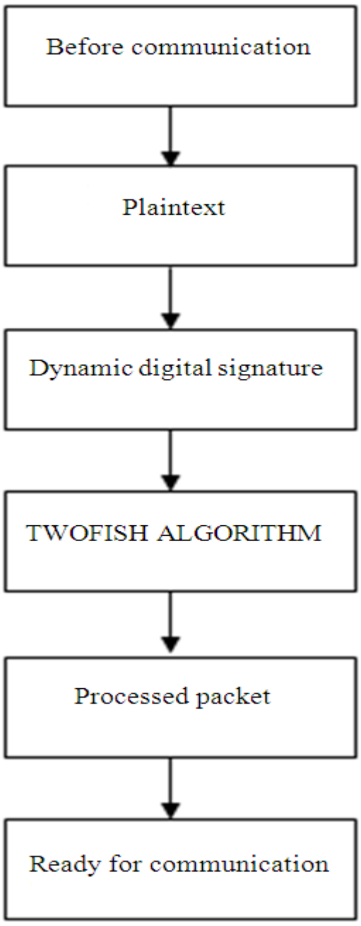

Fig. 3. Work flow diagram for TWOFISH ALGORITHM

There by showing the better performance. TWOFISH ALGORITHM key sizes range from 128 bits to 256 bits. Sybil Attack, DOS attack and wormhole attack can be avoided using the Enhanced EAACK technique. Thereby better performance and low overhead is achieved. The simulation parameter is mentioned in the Table 1.

Algorithm for S-EAACK

```
1. Start→S
2. Before: Commn;(communication)
        Packet $P_k$→Start
         i) Sender→(Dy (sign + $P_k$) + Tf); (dynamic digital signature, twofish)
         ii) Receiver→($D_c$ + $S_k$); (Decryption, secret key)
         iii) Ack→sender; (Acknowledgement)
3. Step 2 is continuing until all packets have been delivered
4. Stop
```

Scheme Description

Inthis section, we describe our proposed secured Enhanced Adaptive Acknowledgement (S-EAACK) scheme using TWOFISH ALGORITHM. The approach described in this research paper is based on our previous work (Shakshuki *et al*., 2013), where the backbone of EAACK was added and evaluated using digital signature through implementation. In this study, we extend it with the introduction of TWOFISH ALGORITHM to prevent the attacker from the acknowledgement packets and deliver a better performance.

Dynamic Digital Signature and TWOFISH ALGORITHM

In order ensure the communication process to be safe and secure,we introduce dynamic digital signature scheme using TWOFISH ALGORITHM, for this, we implemented both DSA and RSA dynamic digital signature using TWOFISH ALGORITHM. Hence the sender and receiver communication processshould be protected from various attacks and vulnerabilities,inturn better network performance is gained.

Figure 3 Depicts the work flow process of TWOFISH ALGORITHM in detail, before the packet is sent for communicationthe packet should be signed using dynamic digital signature. This plaintext is wrapped with dynamic digital signature, then it is incorporated with TWOFISH ALGORITHM, this TWOFISH ALGORITHM is processed in various stages which include Input whitening, further it is followed from first round to fifteen rounds,therafter the processed packet is ready for communication. Using Table 1 simulation parameter we have obtained the results and graphs are plotted with regard to it asshown in the Fig. 4-6 respectively.

Simulation Parameters

The Table 1 shows the parameters taken to execute the proposed algorithm.

Table 1. Simulation parameter

Simulator	NS2
Simulation time	10(s)
No. of mobile nodes	50
Topology	500m*500m
Transmission range	250m
Routing protocol	EAACK
Maximum bandwidth	2Mbps
Traffic	Constant bit rate
Maximum speed	10000 µs
Pause time	2(s)

Scenario 1: Delay

In Figure 4, Delay is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. This includes all possible delays caused by buffering during route discovery latency queuing at the interface queue. The results are shown in the graph:

Formula for Average End to End delay=S/N

where, 'S' is sum of the time spent to deliver packets for each destinationand 'N' is the number of packets received by all the destination nodes. By using Table 1parameter the graphs are obtained with the help of NS2.

Scenario 2: Energy

In Figure 5, Energy is defined as the amount of energy spent during the transmission of packet from the source to the destination. It is measured as kilobytes per second. Energy spent for Twofish is lesser than EAACK, so performance metric is comparatively good for Twofish.

Scenario 3: Packet Delivery Ratio

In Figure 6, Packet Delivery Ratio (PDR) is defined as the ratio of data packets received by the destinations by those generated by the sources:

Packet Delivery Ratio (PDR) = S1/S2

where, 'S1' is the sum of data received by the destination and 'S2' is the data packets generated by each source. Consider the network consists of 50 nodes and transmission takes place to all the nodes in the network. Using EAACK method, the packet delivery ratio is shown in the graph with respect to the attack and the results are shown in graph.

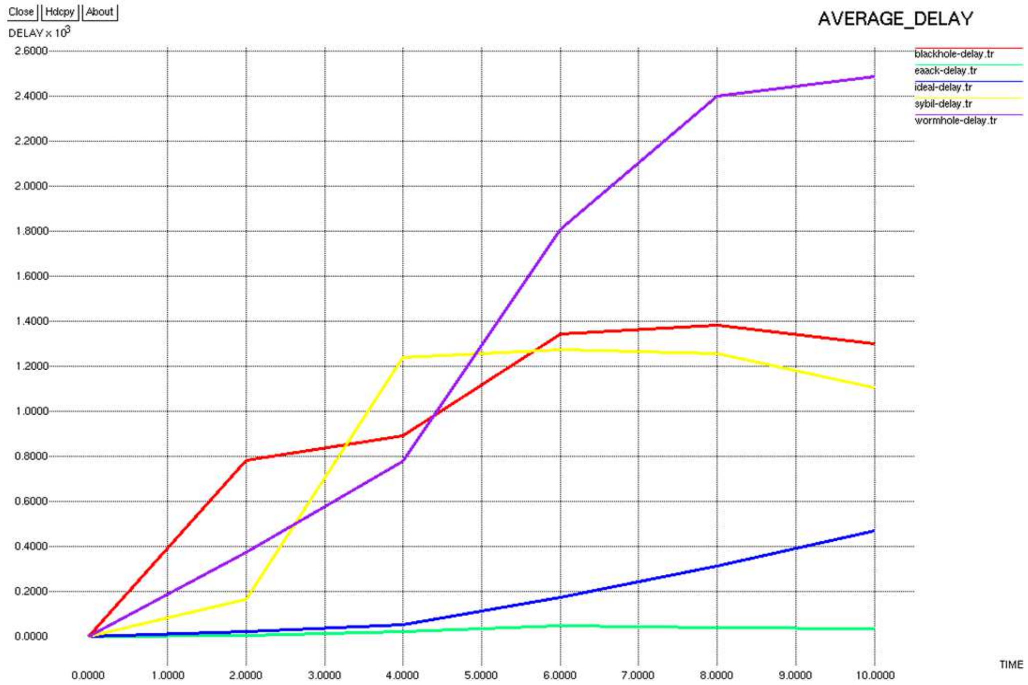

Fig. 4. Delay graph

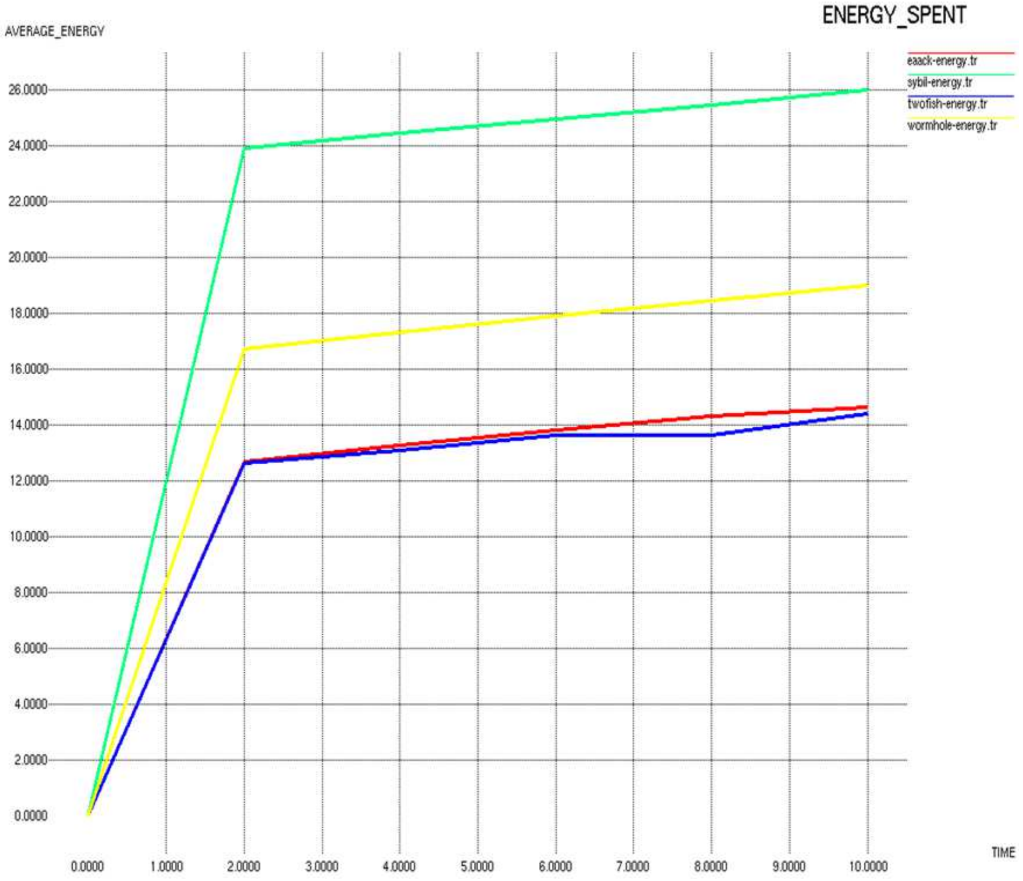

Fig. 5. Energy GRAPH

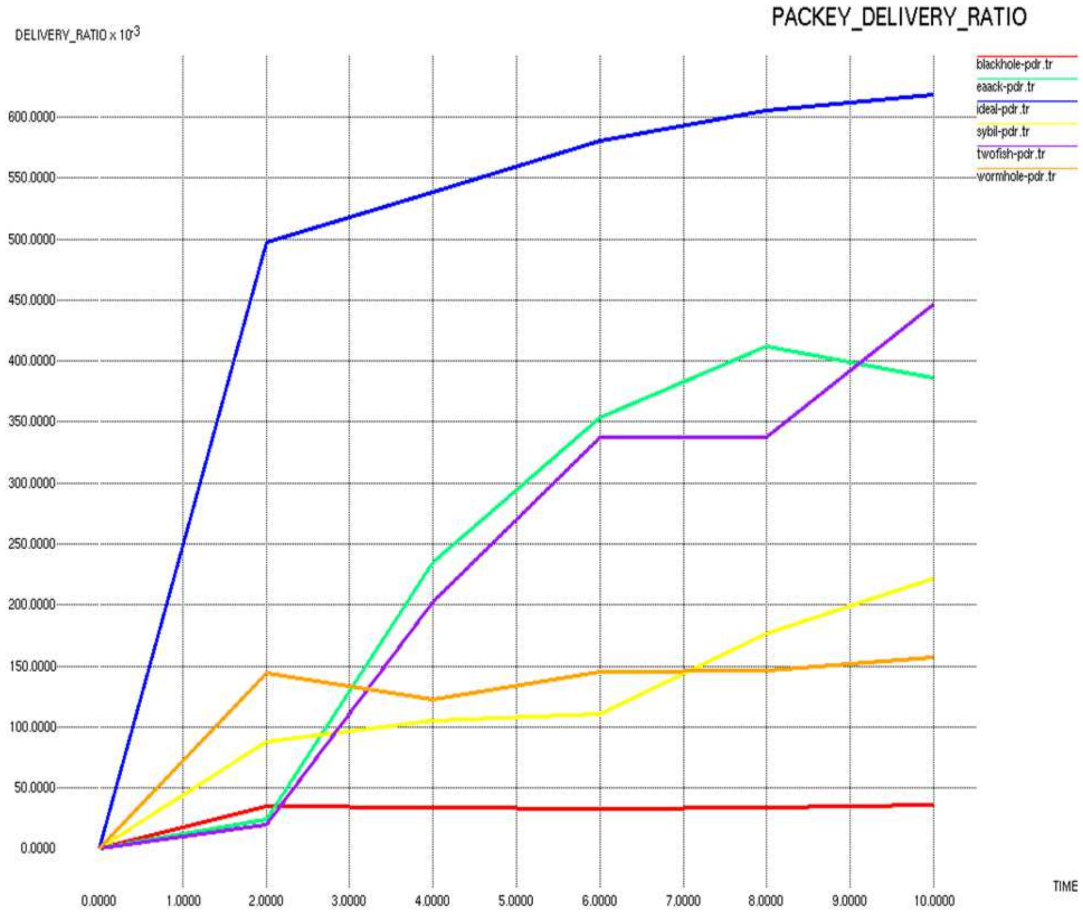

Fig. 6. Packet delivery ratio graph

Conclusion

Packet-dropping attack has always been a major threat to the security in MANET's. In this research paper, we have proposed novel IDS named S-EAACK with dynamic digital signatures using TWOFISH ALGORITHM. This algorithm is used to enhance the network performance parameters such as end-to-end delay, throughput, packet delivery ratio and energy spent calculation (the output is shown in graphs). The performance results are better when compared to EAACK and Our future work is to improve the QOS in MANET's by using hybrid cryptography techniques.

Acknowledgement

The authors wish to thank anonymous reviewers for their valuable, detailed comments that improve both the content and representation of this study.

Funding Information

The authors have no support or funding to report.

Author's Contribution

All authors equally contributed in this work.

Ethics

This article has not published in any journal so far and the co-author is the guide of the corresponding author under whose concurrence it is proposed to get it published through this publishing house.

References

Bhalaji, N.S., 2008. A novel routing technique against packet dropping attack in adhoc networks. J. Comput. Sci., 4: 538-544. DOI: 10.3844/jcssp.2008.538.544.

Johnson, D.B. and D.A. Maltz, 1996. Dynamic Source Routing in Ad Hoc Wireless Networks, In: Mobile Computing Chapter 5, Tomasz I. and H.F. Korth (Eds.), Kluwer Academic Publishers, Springer US. ISBN-10: 978-0-7923-9697-0, pp: 153-158.

Liu, K., J. Deng, P.K. Varshney and K. Balakrishnan, 2007. An acknowledgment-based approach for the detection of routing Misbehavior in MANENT's. IEEE Trans. Mobile Comput., 6: 536-550. DOI: 10.1109/TMC.2007.1036

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th International Conference on Mobile Computing and Networking, Aug. 06-11, ACM, New York, USA, pp: 225-65. DOI: 10.1145/345910.345955

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Communications, 21: 120-126. DOI: 10.1145/359340.359342

Shakshuki, E.M., N. Kang and T.R. Sheltami, 2013. EAACK-a secure intrusion-detection system for MANETs. IEEE Trans. Indust. Electron., 60: 1089-1098. DOI: 10.1109/TIE.2012.2196010

Sheltami, T., A. Al-Roubaiey, E. Shakshuki and A. Mahmoud, 2009. Video transmission enhancement in presence of misbehaving nodes in MANENT's. Int. J. Multimed. Syst., 15: 273-282. DOI: 10.1007/s00530-009-0166-0

Yang, L., 2011. Distance-preserving dimensionality reduction. Wiley Interdisc. Rew, Data Mining Knowledge Discovery, 1: 369-380. DOI: 10.1002/widm.39

Zhang, Y., W. Lee and Y. Huang, 2003. Intrusion detection techniques for mobile wireless networks. ACM Kluwer Wireless Netw. J., 9: 545-556. DOI: 10.1023/A:1024600519144.