Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1178 – 1190

RESEARCH ARTICLE

ID SECURITY SYSTEM IN HIGH TRAFFIC FOR MOBILE ADHOC NETWORK USING ACKNOWLEDGEMENTS

Asha N[1], Gowtham M[2]

1. Assistant Professor, Department of PGS-CEA, National Institute of Engineering, Mysore-570 008
2. II[nd] year M-Tech, Computer Network Engineering, National Institute of Engineering, Mysore-570 008

Abstract : With the various and increasingly malicious attacks on networks and wireless systems, traditional security tools such as anti-virus programs and firewalls are not sufficient to provide free, integrated, reliable and secure networks. Intrusion detection systems (IDSs) are one of the most tested and reliable technologies to monitor incoming and outgoing network traffic to identify unauthorized usage and mishandling of computer system networks. It is critical to implement intrusion detection systems (IDSs) in computer networks that have high traffic. Due to the fact that software IDSs are able to detect all the growing threats to high-speed environments, such as flood attacks or Denial and Distributed Denial of Service Attacks, because the main function of these kinds of attacks is simply to send more traffic in high speed to systems to stop or slow down the performance of systems. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure. Every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. In this paper, we propose and implement a hybrid cryptography technique of diffie hell man key exchange algorithm with new energy constraint based intrusion-detection system named two tier Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

Index terms : Network Security, Open Source, IDS, Enhanced Adaptive ACKnowledgment (EAACK), Mobile Ad hoc NETwork (MANET)

1. INTRODUCTION

Mobile Ad hoc NETwork (MANET) 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. Industrial remote access and control via wireless networks are becoming more and more popular these days . One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [10]. MANET is capable of creating a self configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET 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 [16]. Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry [14]. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, 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 [5], attackers can easily compromise MANETs by inserting malicious or noncooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS).

Security is a major concern in every aspect of our daily life. New methods and equipment have been devised to ensure privacy. However, computer networks still face many threats [1]. There are usually three stages to achieving security in computer system networks: prevention, detection and correction [2]. Prevention is preferable to detection and correction, but it is impossible to prevent 100 per cent of attacks [1, 3]. Moreover, detection techniques provide more accurate results in detecting malicious attackers than correction techniques. Despite the existence of a variety of security protection measures, an attacker often attempts to make services merely unavailable to intended legitimate users [3]. It is inadvisable to depend only on prevention techniques, especially when an attacker has successfully obtained vulnerable information from a network, but prevention can successfully and effectively restore a network before an attack is launched. Correction techniques are adopted to protect computer systems. Along with prevention, they actively work to block intrusions, but can continue to battle a successful intrusion. Nevertheless, a

number of successful attacks can be controlled using prevention techniques if an attack is detected at the interim stage of prevention systems. This is difficult, because some successful attacks can get through the prevention system [1]. It is a matter of a system being attacked, compromised, and consequently malfunctioning. Here we need an interim stage such as the detection phase, which should be positive during intrusions. Therefore, the detection method is preferred to minimize network costs and fill in the gap between correction and prevention mechanisms.

Intrusion Detection (ID) is one of the most tested and reliable technologies to monitor incoming and outgoing network traffic to identify unauthorized usage and mishandling of computer system networks [3, 4]. In addition, ID identifies the activity of malicious attackers. Due to the fact that numerous computer systems are unable to prevent threats such as flood attacks, DoS(denial of service) attacks affect many systems, because the impact of such attacks is severe and irrevocable. The main function of these kinds of attacks is to send more high-speed traffic to a network address, which stops or slows down the performance of legitimate users' computer network systems by exploiting vulnerabilities such as misconfigurations and software bugs generated from internal and external networks. It is critical to implement ID systems (IDSs) in computer networks that have high traffic . IDSs consist of either software applications or hardware to listen for and detect malicious activities at the gateways (incoming and outgoing) of individual or network systems.

2. BACKGROUND

2.1 **Security Products:** Security products such as firewalls and antivirus programs are less efficient than IDSs and have different functionalities. IDSs analyse collected information and infer more useful results than other security products. The difference between IDSs and security products such as antivirus programs is that, while IDSs require more intelligence than security product software, they analyse gathered information and deduce useful results [1].

2.1.1 **Firewall Technology**

Network traffic is usually filtered according to criteria such as origin, destination, protocol and service, typically through dedicated routers called firewalls [1]. The functionality of the firewall is based on filtering mechanisms specified by a set of rules, known as a policy, which can protect a system from flooding attacks [1]. The basic operation of firewalls is to filter packets passing through specific hosts or network ports, which are usually open in most computer systems [1]. It does not perform deep analysis (malicious code detection in the packet) and treats each packet as an individual entity [1]. The disadvantage of a firewall is that it cannot fully protect an internal network; it is unable to stop internal attacks [1, 6]. For example, malicious and unwanted web traffic can go through a firewall to strike and damage a protected computer system without a hitch.

2.1.2 **Anti-virus technology**

Computer viruses are programs which cause computer failure and damage computer data. Especially in a network environment, a computer virus poses an immeasurable threat and can be very destructive [6]. The functionality of an anti-virus program is a running process that examines executables, worms and viruses in the memory of guarded computer/network systems instead of monitoring network traffic. Although an anti-virus program monitors the

integrity of data files against illegal modifications, it is unable to block unwanted network traffic intended to damage the network. [7].

2.1.3 **IDS technology**

Firewalls have been used for network security for a long time, but they can be easily bypassed, as a lot of techniques for deceiving firewalls have been developed [8]. IDSs are much more advanced and enhanced security tools than firewalls, because a firewall just drops packets—it cannot detect intrusion [1]. In addition, it is difficult to detect suspicious activities in the midst of high traffic and other such adverse circumstances in the network, which results in an inaccurate detection mechanism. IDSs are still unable to control all threats and malicious activities [1, 9]. To overcome such design and implementation difficulties, novel IDS outcomes have been obtained from multiple characteristics of advanced computer networks: Processing in real time; High speeds and high loads; Reducing difficulties for defenders; and Increasing difficulties for attackers. The specialized IDS mechanism is based on how, where and what it detects, along with mandatory requirements. In particular, IDSs should be based on flexible and scalable network components to accommodate the drastic increase in today's network environments. They should provide straightforward management and operational procedures and steps rather than complicating underlying tasks, and they should provide user-friendly ID mechanisms.

2.2 **IDS in MANETs**

As discussed before, due to the limitations of most MANET routing protocols, 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, an 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 the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches. Anantvalee and Wu [4] presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK [15], and Adaptive ACKnowledgment (AACK).

2.2.1 **Watchdog:** Marti *et al.* proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Path rater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious

nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme [15]. Nevertheless, as pointed out by Marti *et al.* [16], the Watchdog 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; and 6) partial dropping.

2.2.2 **TWOACK:** With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu *et al.* [16] is one of the most important approaches among them. On Fig. 1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it. The contrary to many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment 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 (DSR) [11]. The working process of TWOACK is shown in Fig. 1: Node X first forwards Packet 1 to node Y, and then, node Y forwards Packet 1 to node Z. When node Z receives Packet 1, as it is two hops away from node X, node Z is obliged to generate a TWOACK packet, which contains reverse route from node X to node Z, and sends it back to node X. The retrieval of this TWOACK packet at node X indicates that the transmission of Packet 1 from node X to node Z is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes Y and Z are reported malicious. The same process applies to every three consecutive nodes along the rest of the route. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

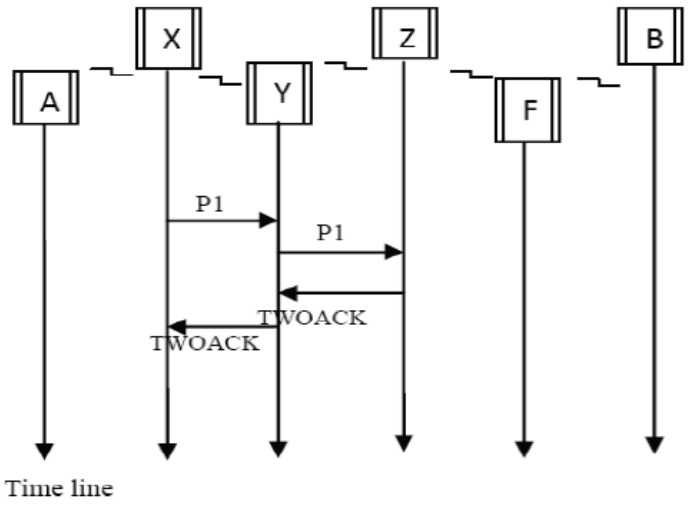

Fig 1: TWOACK IDSs for MANETs

2.2.3 AACK*:* Based on TWOACK, Sheltami *et al.* proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The end-to-end acknowledgment scheme in ACK is shown in Fig. 2. In the ACK scheme shown in Fig. 2, the source node A sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node B receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node A along the reverse order of the same route.

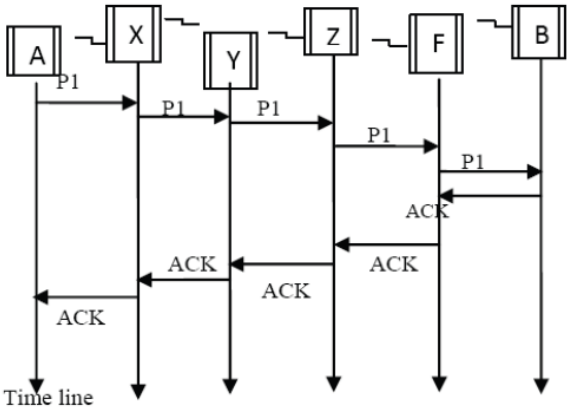

Fig 2: END-to-END ACK IDS for MANETS

Within a predefined time period, if the source node A receives this ACK acknowledgment packet, then the packet transmission from node A to node B is successful. Otherwise, the source node A will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, 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. In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK).

3. EXISTING SYSTEM

3.1 **ACK**

As discussed before, ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In ACK mode, node A first sends out an ACK data packet P1 to the destination node B. If all the intermediate nodes along the route

between nodes A and B are cooperative and node B successfully receives P1, node B is required to send back an ACK acknowledgment packet ACK along the same route but in a reverse order. Within a predefined time period, if node A receives ACK, then the packet transmission from node A to node B is successful.

Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

3.2 **S-ACK**

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu et at. The 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.

S-ACK mode, the three consecutive nodes (i.e., X , Y, and Z) work in a group to detect misbehaving nodes in the network. Node X first sends out S-ACK data packet Psad1 to node Y. Then, node Y forwards this packet to node Z. When node Z receives Psad1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet Psak1 to node Y. Node Y forwards Psak1 back to node X. If node X does not receive this acknowledgment packet within a predefined time period, both nodes Y and Z are reported as malicious. Moreover, a misbehavior report will be generated by node X and sent to the source node A. Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report,

EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

3. 3 **MRA**

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge

4. **PROPOSED SYSTEM**

Secure IDS architecture (EAACK) introduced to improve the security level of MANETs based on security attributes and various algorithms, namely RSA and DSA. EAACK is designed to tackle three out of six weaknesses of Watchdog IDS, namely, 1) Receiver collision, 2) Limited transmission power, 3) False misbehavior.

4.1 **Receiver collisions:** Example of receiver collisions, shown in Fig. 3, after node X sends Packet 1 to node Y, it tries to overhear if node Y forwarded this packet to node Z; meanwhile, node F is forwarding Packet 2 to node Z. In such case, node X overhears that node Y has successfully forwarded Packet 1 to node Z but failed to detect that node Z did not receive this packet due to a collision between Packet 1 and Packet 2 at node Z.

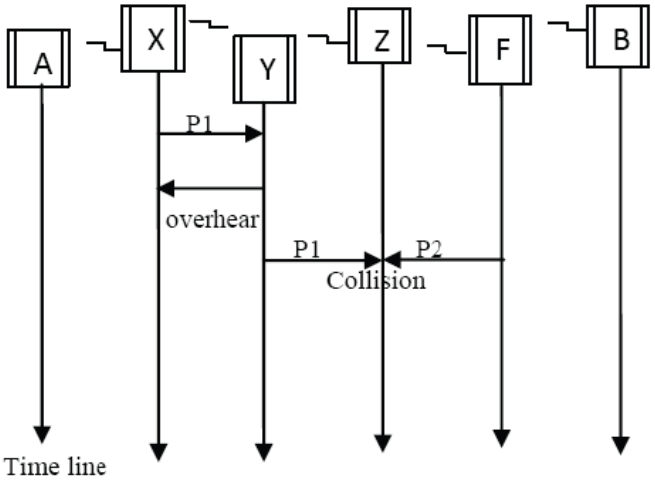

Fig 3: **Receiver collision in MANETS**

4.2 **Limited transmission power:** In order to manage the battery resources in MANETs, node Y limits its transmission power so it is very strong to be overheard by node X after transmitting the packet (P1) to node Z, but too weak to reach node Z because of transmission power can be reduced.

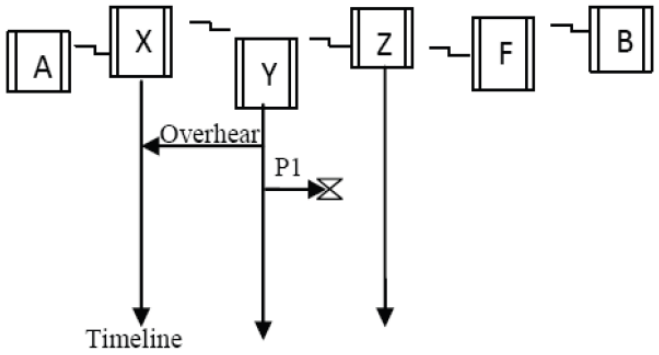

Fig 4: **Limited Transmission Power in MANETS**

3)False misbehavior: Example of false misbehavior in MANETs, shown in Fig. 5, Even though node X and Y forwarded Packet 1 to node Z successfully, node X still inform node Y as misbehaving, as shown in Fig. 5. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack. As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of

them are vulnerable to the false misbehavior attack. In order to solves not only receiver collision and limited transmission power but also the false misbehavior problem to launch Secure IDS architecture.

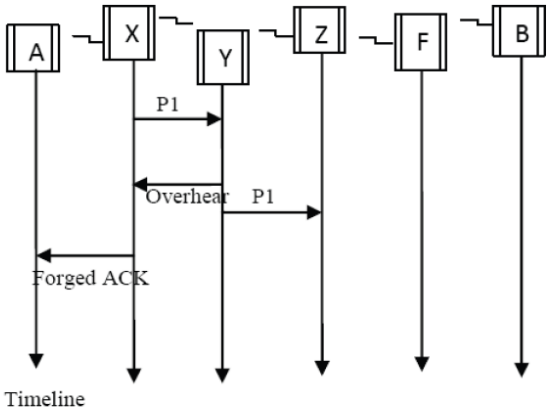

Fig 5: **False Misbehavior in MANETS**

5. Secure IDS description

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes to include a 2-b packet header in EAACK. According to the Internet draft of DSR [7], there is 6 b reserved in the DSR header. In EAACK, use 2 b of the 6 b to flag different types of packets.

Furthermore, for each communication process, both the source node and the destination node are not malicious. All acknowledgment packets are required to be digitally signed by its sender and verified by its receiver.

In this secure IDS, It is assumed that the link between each node in the network is bidirectional.

Furthermore, for each communication process, both the source node and the destination node are not malicious. All acknowledgment packets are required to be digitally signed by its sender and verified by its receiver.

DATA	ACK	S-ACK	MRA

Fig 6: EAACK protocol in MANETS

5.1 **ACK:** ACK is basically an end-to-end ACK IDS. It acts as a part of the hybrid IDS in EAACK, aiming to reduce network overhead when no network misbehavior is detected. Consider the scenario source node first sends out an ACK data packet to the destination node D. If all the intermediate nodes along the route between nodes S and

D are cooperative and node D successfully receives packet, node D is required to send back an ACK acknowledgment packet along the same route but in a reverse order. Within a predefined time period, if node S receives packet, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

5.2 **S-ACK:** It is an improved version of the TWOACK IDS [6]. The 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.

TABLE 1: **Packet Type Indicator**

Packet Type	**Packet Flag**
General Data	00
ACK	01
S-ACK	10
MRA	11

The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

5.3 **MRA :** Unlike the TWOACK IDS, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior. The MRA field is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. The core of MRA field is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

5.4 **Digital Signature**

As discussed before, EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors 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. Hybrid cryptography technique Diffie Hellman key exchange algorithm is used reduce the network overhead.

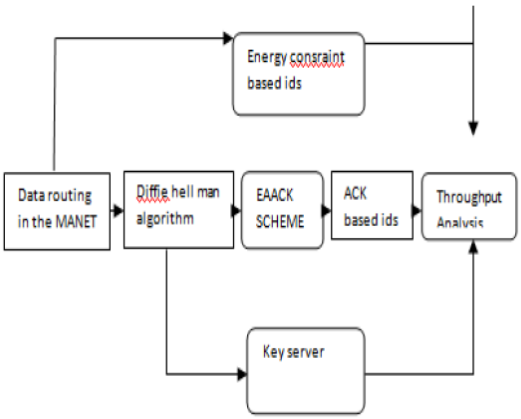

Fig 7: **Diffie Hellman Cryptography in MANETS**

6. CONCLUSION

Intrusion- Detection Systems (IDS) for discovering malicious nodes and attacks on MANETs is presented. Due to some special characteristics of MANETs, prevention mechanisms alone are not adequate to manage the secure networks. In this case detection should be focused as another part before an attacker can damage the structure of the system. Secure IDS named EAACK protocol specially designed for MANETs and in future it is required to compare against other popular mechanisms. Security is major part in MANETS, hybrid architecture will tackle the issue in an efficient manner. This way we can better preserve battery and memory space of mobile nodes.

AUTHORS

1) **ASHA N**

Assistant Professor, Department of PGS-CEA, National institute of engineering, Mysore**.**

Email-id: **ashan_usha@yahoo.com**

2) **GOWTHAM M**

M-Tech in Computer Network Engineering, Department of PGS-CEA at National Institute Of Engineering, Mysore.
Email-id: **gouthamgouda@gmail.com**

REFERENCES

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

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

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer- Verlag, 2008.

[5] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582,2007.sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3 13.

[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[10] G. Jayakumar and G. Gopinath,

[11] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[13] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[14] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[15] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[16] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007. 28, 2007, pp. 1154–1159.

