International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 7 Issue 1 –APRIL 2014.

Secure Transmission of Packets using EAACK in MANETs

Mrs.K.Esther[1], K.Sathish[2], K.Balamurugan3 and A.Udhayakumar[4]
Asst Prof, Dept of ECE, Dr.SJS Paul Memorial College of Engineering and Technology
UG, Dept of ECE, Dr.SJS Paul Memorial College of Engineering and Technology

ABSTRACT:

The Mobile Ad Hoc Network (MANET) is the collection of mobile nodes that consists of both the transmitter and receiver to communicate with each other through wireless links. MANET is capable of creating self configuring and self maintaining network. The Intrusion Detection System (IDS) is implemented for detecting the malicious nodes misbehavior in the network. The false misbehavior report is acknowledged to the source node by using the Enhanced Adaptive Acknowledgement (EAACK), and no transmission takes place through the particular node. In this paper, we proposed to rectify the detected malicious nodes and allow transmission through those nodes. Hybrid cryptographic technique is also adopted for secure transmission and further to reduce the network overhead and increase packet delivery ratio.

Index Terms—**Digital signature, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgement (EAACK), Mobile Ad Hoc Network (MANET), Intrusion Detection System (IDS).**

I.INTRODUCTION

MANET is a type of multi-hop network, infrastructure less and most important is self organizing. One of the main characteristics of MANET's with respect to security point of view is lack of clean line defense. This has the dedicated routers which perform routing functionalities for devices but in case of Mobile Ad Hoc Network are concerned each other mobile nodes act as router and forward packets to each other nodes. It is known that wireless channel is accessible to both network users as well as to the attackers. In this since there is no infrastructure exists and network topology changes in an unpredictable manner since nodes are free to move. The main communication medium is broadcast. Nodes can be regarded as wireless mobile hosts with short term power supply, a relatively short communication range, low processing power and limited bandwidth. MANETs also use Personal Digital Assistants (PDA) for the purpose of communication. These networks are generally dynamic collections of self organizing mobile nodes with links that are characterized by the dynamic topology changes and no fixed infrastructure. This is in contrast to well-known single hop cellular network model that supports the needs of wireless communication by installing base stations as access points. The current Mobile ad hoc networks allows for many different types of attacks. Although analogous exploits also exists in wired networks but it is easy to fix by infrastructure in such a network. This type of network is based on the cellular architecture in which a large area to be covered is divided into several cells, each having a fixed base station. Each cells consists of several Mobile Terminals (MT) which communicate to other mobile terminal in the same cell through the base station. Current MANETs are vulnerable to two different types of attacks, namely active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. Passive attacks are mainly due to lack of cooperation with the purpose of saving energy. A group of malicious nodes can collude in attacking the network causing for more damage than a single node. In general if keying material is compromised or a malicious node collude with others to intentionally disrupt communications the extent of damage increases with the number of colluding adversaries and availability of keying material. The traditional routing protocol that has been used in the design of wired network cannot be used in the wireless network due to highly dynamic nature of mobile nodes as well as non-existence of a central authority for over all control.

The major challenges facing the design of mobile ad hoc routing protocols are the nodes mobility, resource constraints such as power and bandwidth as well as unstable channel states. Due to the nature of mobile nodes which can be highly dynamic, communication between mobile nodes is often characterized by frequent path breaks and reconnections. The power usage by routing protocols will have an impact on the overall performance [2]. Here a node is the sole router linking two independent networks. If any unnecessary usage of power on this node will further drain powers it and thereby causes a link breakage between the two networks when the node runs out of power [7]. Besides power bandwidth is also scare commodity in the MANET environment. A receiver can receive simultaneous data from different senders, which are totally out of range from each other. As such they do know that different party is sending data to the sender at the time. As the number of nodes increase this problem can be aggravated. Other issues include limited physical security for mobile ad hoc nodes. Since the nodes are not statically located they are prone to more physical security threats than fixed routers [8]. Compromised nodes may pose serious problem to the entire network, it is possible to use them especially as devices to deviate data traffic or launching pad for attack against other nodes. Unlike typical wired link routers the power source of nodes comes from non permanent power sources such as batteries. A good routing protocol must be scalable and robust enough for rapid building and tearing down of routes.

II.INTRUSION DETECTION SYSTEM (IDS)

The Intrusion Detection System should be added in MANETs to enhance the security levels. The potential damages that are caused by the compromised nodes can be eliminated in MANET as soon as the attackers enter the network. With a limited mobility collaborative IDSs will perform best in the densely populated MANET and worse in sparsely populated MANET [3]. This is a great complement to the existing proactive approaches. To protect the individual nodes and to defend the Mobile Ad Hoc Networks from malicious attackers intrusion detection and response mechanisms are needed. We detect intrusions by neighboring nodes from their deviation from known or expected behavior. When nodes act as forwarding nodes, offering routes to other destinations it is expected that those nodes actually forward data packets. Nodes are expected to retransmit the message without modifying payload towards the intended recipients. The IDS also should allow monitoring of packet traffic for specific protocols. Intrusion system makes use of predictable pattern in those specific protocols to spot abnormal behavior, and in some instances specific signatures indicating malicious activity.

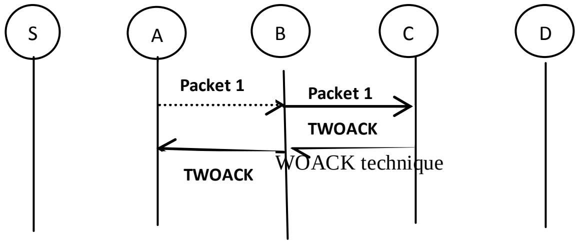
The packets are transmitted from one node to the other. It has to be transmitted within the predefined threshold time, in case if exceeding this threshold time a failure count is increased and the node is reported as misbehaving node [10]. Thus after the misbehaving nodes are detected, the packets through those nodes are dropped. In this no false misbehavior report is intimated to the source node. Here detection of infected nodes may reduce the impact of misbehavior, but it does not totally eliminate the impact of misbehavior. To perform this the following ways such as blacklisting and eliminate them from all routes may be carried out. There are also two types of approaches are carried out for the detection of the malicious nodes, namely centralized approach and localized approach [6]. The global knowledge is assumed for centralized approach and local knowledge is assumed for the localized approach for the routes. The localized approach is better since it is self organizing, decentralized nature of ad hoc networks. Limited range wireless communication and mobility means that the nodes must cooperate with each other to provide essential networking, with the underlying network dynamically changing to ensure needs are continually met. The dynamic nature of the protocols that enable MANET operation means they are readily suited to deployment in extreme or volatile circumstances. There are three main components of IDS: data collection, detection and response. The data collection component is responsible for collection and pre-processing data tasks : transferring data to a common format, data storage and sending data to the detection module. Intrusion detection system can use different data sources as input to the system: system logs, input packets etc., In the *detection component* data is analyzed to detect intrusion attempts and indications of detected intrusions are sent to the response component. In the literature, three intrusion detection techniques are used. The first is anomaly-based intrusion detection which profiles the symptoms of normal behaviors of the system such as usage frequency of commands, CPU, usage for programs and the like.

In this section, we describe three main approaches, namely, Watchdog, TWOACK, Adaptive ACKnowledgement (AACK).

1) Watchdog: The aim of the watchdog is to improve the throughput of network with the presence of malicious nodes. Thus as we have discussed if a watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases the failure counter. Whenever a node’s failure counter exceeds the given predefined threshold, the watchdog reports it as misbehaving. Here the pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. The research studies and implementations have proved that the watchdog scheme is efficient. This is capable of detecting malicious nodes rather than links. These advantages have made watchdog scheme a popular choice in field.

2) TWOACK: It is one of the most important approaches on 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 destination. It is required to work on routing protocols such as Dynamic Source Routing (DSR). Here the packet is transmitted from the node S to node A. Then node A transmits to the next node B. Node B sends the packet to node C. The C node sends an

TWOACK acknowledgement packet to the node A, since node C is two hops away from the node A. Thus if the TWOACK packet is not received within the predefined time period, then both the nodes B and C are reported malicious.



WOACK technique

3) AACK: It is also an acknowledgement based network layer scheme which is similar to the TWOACK scheme. Compared to TWOACK, AACK significantly reduces the network overhead which still capable of maintaining or even surpassing the same network throughput. For the packet transmission from the source node to the destination, the acknowledgement packet must be received within a predefined time, or else it is detected as malicious.

III. DIGITAL SIGNATURE ALGORITHM

Digital Signature Algorithm (DSA) is a cryptographic technique related to information and data security such as privacy, reliability, and substantiation. In this method a message is encrypted using the public encryption key. The message hash function is created and sent from the receiver to the destination. The receiver must get the private key of the sender to decrypt the message for further use. It is widely provided to ensure the authentication, integrity, and non repudiation of MANETs. Thus it is more efficient to the EAACK system in MANET, since it provides more security.

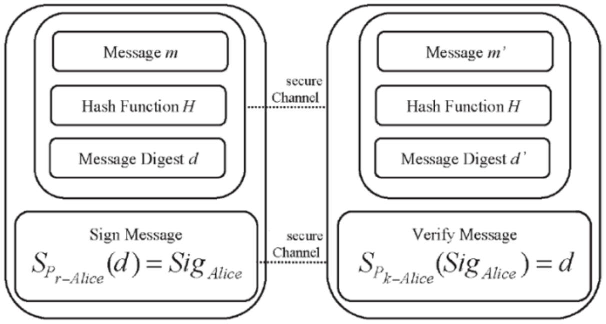


Fig 2.Secure channel communication

The flow of communication through the digital signature is given above. The message with fixed length *m* is computed through the hash function *H*. The sender has its own private key Pr_{send} on the digest message *d*. Now the signature with Sig_{send} is attached with the message *m*. The sender always keeps the private key as secret and does not reveal it to anyone[9]. Because if the attacker gets the secret key, then it can easily grasp the messages from the sender which is signed by the sender. So the malicious attacker may affect the entire network.

Since the messages are digitally signed by the sender, the receiver sees those messages as reliable and substantiated. The sender sends the message *m* with the digital signature Sig_{send} trough the secure channel. In this secure channel the intrusion detection agent is implemented to every node to detect the malicious attackers. Then the message *m* sent by the sender needs a process to be obtained by the receiver. The sender reveals a public key $P_{k,}$ on the signature of the sender Sig_{send}. Thus by obtaining this public key the receiver gets the private provided by the sender to read the information .

The intrusion acknowledgement, two-Ack acknowledgement, and intrusion watchdog are three acknowledgements that are used here for the malicious vs overhead process. In this as soon as the malicious attacker interrupts, an intrusion acknowledgement is intimated to the source node. The watchdog here detects the malicious behavior by clearly watching the next hoping transmission time. If the packet transmission takes the time more than the predefined threshold time then the node is reported as malicious, and the packet loss occurs here. Here also occurs the other problem such as receiver collisions, packet dropping and the limited transmission power [13]. This also reflects as the problem of packet delivery ratio and more routing paths which consume more power.

Homomorphic Encryption

Homomorphic encryption is a form of encryption which allows specific type of computations to be carried out on cipher text and generate an encrypted result which, when decrypted, matches the result of operations performed on the plain text. This is a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services. There are several efficient, partially homomorphic cryptosystems and a number of fully homomorphic but less efficient cryptosystems. Although a cryptosystem which is unintentionally homomorphic can subject to attacks on this basis, if treated carefully, homomorphism can also be used to perform computations securely.

The utility of fully homomorphic encryption has been long recognized. The problem of constructing such a scheme was first proposed within a year of development of RSA. A solution proved more elusive and it was unclear whether fully homomorphic encryption was possible. The best result was Boneh-Goh-Nissm cryptosystem which supports evaluation of an unlimited number of addition operations.

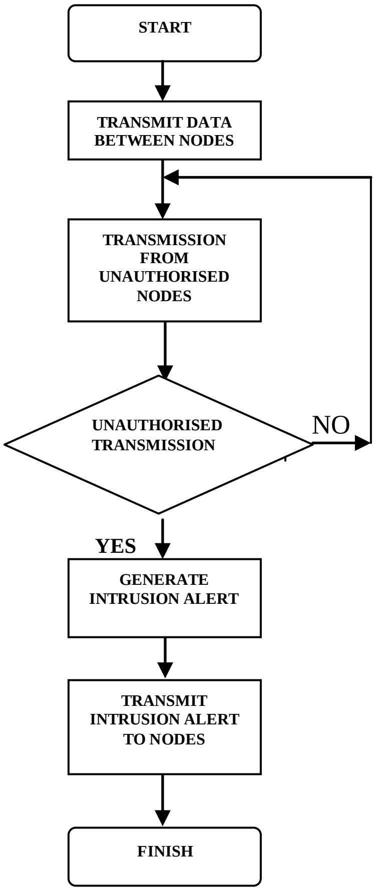

START
TRANSMIT DATA BETWEEN NODES
TRANSMISSION FROM UNAUTHORISED NODES
UNAUTHORISED TRANSMISSION
NO
YES
GENERATE INTRUSION ALERT
TRANSMIT INTRUSION ALERT TO NODES
FINISH

Fig 3.Flow chart for intrusion alert to the nodes

The above flow diagram gives a clear representation of the intrusion alert to the nodes. In this the initial step is to start the process. Now the data or information to be transmitted is selected for a specific purpose. From the source node the data is transmitted between the different neighboring nodes. In some cases the data's are sent through the unauthorized nodes. The unauthorized transmissions through the nodes are identified using the intrusion alert. After the intrusion alert system is generated, the unauthorized transmission is detected and transmission process is stopped and returned to the source node. Only after when the intrusion alert is not given, the nodes can further transmit the packets. Then intrusion alert is given to all the nodes to avoid the malicious attackers. Then finally the finish stage that comes after the successful transmission of packets. Thus the main advantage of this is that, the packet delivery ratio is increased i.e. packet loss is very much minimized and the routing paths or routing overhead is reduced.

Shortest path routing algorithms have been widely used in today's computer network. Nodes are used for transmission.

In such algorithms, nodes attempt to route packets to their destinations over paths of minimum distance and update the distances periodically to adapt topological and traffic changes. Routing algorithms can be classified into *static, quasi-static*, and *dynamic*. In static routing algorithm the choice of routes is predetermined and fixed for relatively long time period. Dynamic routing algorithm, allows continuous changes in routing decisions to reflect the current traffic and topological changes.

IV. PERFORMANCE EVALUATION

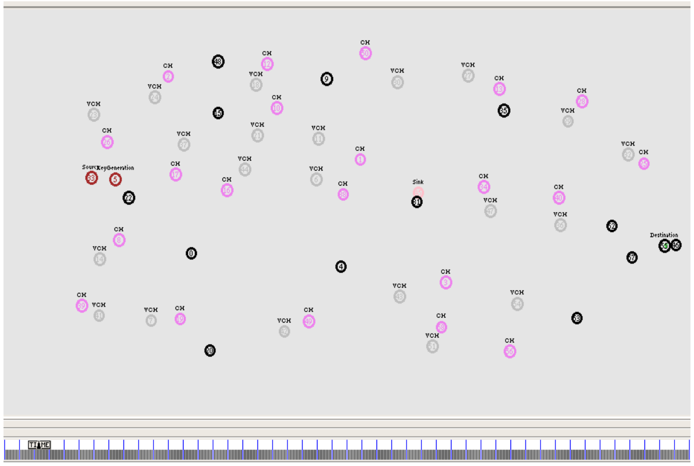


Fig 4.Key generation

The above figure shows the number of nodes used, cluster heads (CH), vice cluster heads (VCH), source and destination. This figure is the proposed model of this paper. The source sends the data packets to be transmitted to the nearby node. Here the original data packet is encrypted and the key is generated. The cluster head stores the data to be transmitted and the copy of data is only transmitted. The purpose of vice cluster head is to only transmit to the nearby routing paths using shortest routing path. The key is generated and transmitted with the packets to decrypt. Since homomorphic algorithm is used the key need not be separately sent to the destination node.

The figure 5 shows that the signaling path is searched through the nearby cluster head and transmitted through the vice cluster head. The attacker comes here to grasp the packets from the vulnerable node. The red node indicates that the node is malicious and the packet drop occurs there. The enhanced adaptive acknowledgement is sent to the source node from the intruded node. Then the malicious node is rectified to normal node. Since the malicious attacker is present, packets are not further transmitted those nodes.

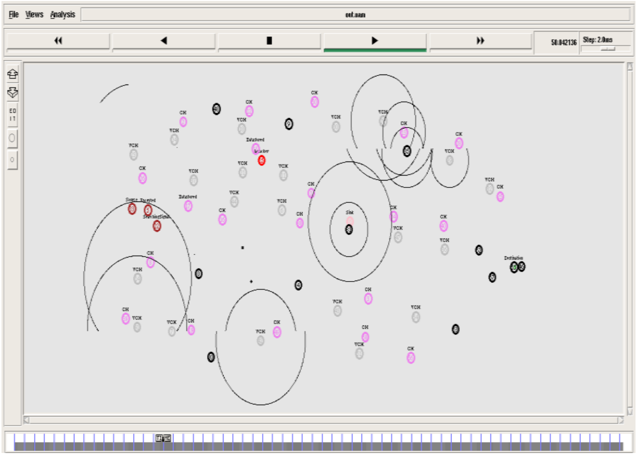


Fig 5.Detection of malicious node

The below figure shows that the packets are transmitted in another routing path through the sink node. The sink node is an intermediate node such as a base station of the mobile network that switches the connection. The circular path present in the figure shows the searching of the communication path for further sending of packets. The sink node transmits to the other cluster to reach the destination. Here at the destination node the encrypted data are decrypted automatically since the homomorphic encryption technique is used. The encrypted data is indicated in blue colour. The destination node sends an acknowledgement to the source node for the successful reception of the data packet. After the transmission is over the copy of the data at each cluster head gets automatically deleted and ready of another packet transmission.

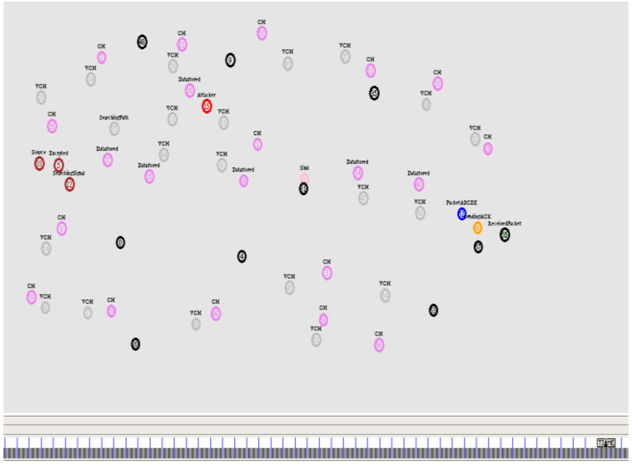


Fig 6.Decryption and acknowledgement to source

The above simulations are done in network simulator (NS2). Routing overhead and packet delivery ratio are the parameters used for analysis.

The graphs shown are the performance analysis of the existing system.

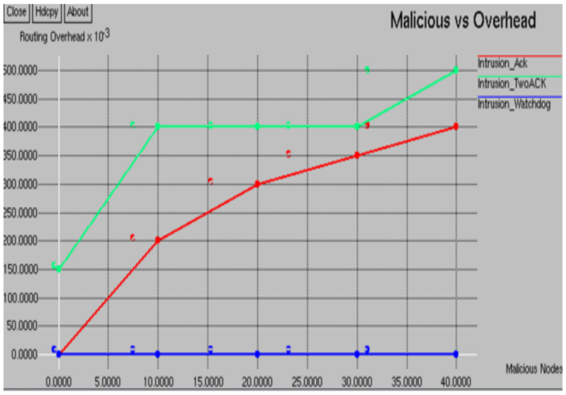


Fig 7. Simulation results for malicious vs overhead

The above graph shows the performance of the malicious nodes and the routing overhead. It also shows the intrusion acknowledgement, intrusion two-acknowledgement, intrusion watchdog. As the intrusion occurs in any of the nodes the acknowledgement is sent to source node. The routing path is increased with the increase in malicious nodes. The malicious nodes are rectified and used as true node.

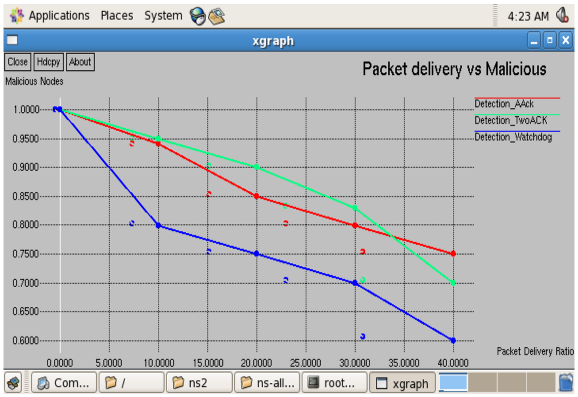


Fig 8. Simulation results for packet delivery ratio vs malicious

The given graph clearly shows that as there is increase in the number of malicious nodes then the packet delivery ratio at the destination is decreased. The detection of AAck, and detection of two-Ack and the detection of watchdog is shown. The above performances are carried out through the Network Simulator.

The upcoming performances are the working of the proposed system. The proposed system also consists of the parameters of routing overhead and the packet delivery ratio with the malicious behavior of nodes.

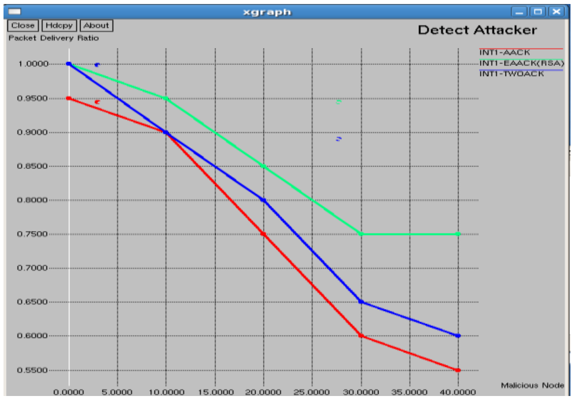


Fig 9.EAACK packet delivery ratio vs malicious

The above graph shows the performance of the packet delivery ratio with the presence of the number of malicious nodes. Here the other two techniques of AACK and TWOACK does not perform better to transmit the packets in the presence of many malicious attackers. But in case of EAACK system though there are many malicious attackers present, the packet delivery ratio exceeds more than compared to the other two techniques. The EAACK transmission is indicated in green colour. The x-axis consists of the malicious nodes and the y-axis consists of the packet delivery ratio.

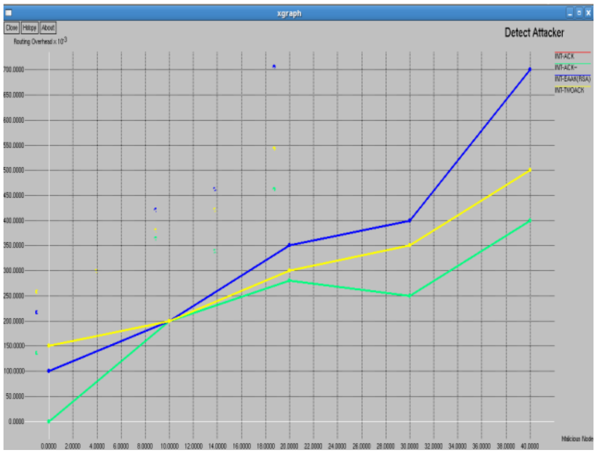


Fig .Routing overhead vs malicious

The above graph shows the performance carried out for the routing overhead and the malicious nodes. The x-axis is given for the number of malicious nodes present and the y-axis is given for the routing overhead. Blue line is EAACK, yellow is TWOACK and green is AACK. The other two techniques of AACK and TWOACK does not perform better since the routing overhead is less with the increase of malicious nodes. The concept is that where there is more routing overhead, there is better performance. In the proposed, as the malicious attacker is present, the new routing path is chosen and the transmission takes place. So the routing overhead increases in order to securely transmit the packets.

V. CONCLUSION AND FUTURE WORK

Packet dropping is one of the major problems that is faced in MANETs. We use the digital signature algorithm for the secure transmission of information. The power consumption is less and it is more efficient. Here the IDS system is implemented to detect the malicious nodes. In our paper, we detect the malicious nodes and rectify those nodes. So that the same node can be used instead of neglecting it. It also increases the packet delivery ratio to the destination and decreases the packet loss.

Unattended wireless sensor network (UWSN) faces challenges in providing good security and in showing good performance The lack of communication with the final data in receivers is the main reason for this. It is possible for UWSN to gather the sensible data for long time. These data's are vulnerable to the adversaries who can compromise the sensor and maneuver the sensed data. This describes how various methodologies are used to act against the adversary troubling the USWNs

The various cryptographic measures have to take the vulnerabilities into consideration, thus making the network to improve its performance and security. In this survey paper, a detailed study about the various schemes that increases the efficiency and performance of UWSNs and the measures taken to improve forward security.

REFERENCES

[1] G. Jayakumar and G. Gopinath,"*Ad hoc* mobile wireless network Routing protocol-A review,"*Comput. Sci, vol 3,2007.*

[11] N. Naseer and Y.Chen,"Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc networks,"in *Proc. IEEE Int Conf,*

[12] A. Patcha and A. Mishra,"Collabrative security architecture for blackhole attack prevention in mobile ad hoc networks,"in *Poc, Radio Wireless , Conf, 2003.*

[13] Nat, Inst. Std. Technol. Digital Signature Standard (DSS) Federal Information Processing Standards Publications, MD, 2009

[14] K.Sathish, Mrs.K.Esther, K.Balamurugan, and A.Udhayakumar, "Reduction of Packet Loss in MANETs using EAACK," in *Proc 1st Int Conf, ICET* ,march 2014

Mrs.K.Esther, works as assistant professor at Dr.SJS Paul Memorial college of Engineering & Technology affiliated to Pondicherry university. She had done UG at Mailam college of Engineering and PG at Dr.Pauls college of Engineering. Presented international conference at International Conference on Emerging Technology (ICET) and a national conference.

[2] J.Parker, J.Undercoofer, J.Pinkston, and A.Joshi,"On intrusion Detection and response for mobile ad hoc networks", in *proc IEEE Int conf.Pervasive compute. Commun, 2005.*

[3] N.Kang, E.Shakshuki, and T.Sheltami,"Detecting misbehaving Nodes in MANETs,"in *Proc. 12th Int.Conf,* Paris, Nov 8-2010.

[4] Y.Hu,Perrig, and D.Johnson,"ARIADNE:A secure on demand routing protocol for ad hoc network"in *Proc* .8th *Int Conf .Mobi com,2002.*

[5] K.Liu, J. Deng, P.K.Varshney, and K.Balakrishnan,"An acknowledgement based approach for the detection of routing misbehavior in MANETs,"*IEEE* Trans.Mobile comput,vol 6,2007.

[6] Y.Hu, A.Perrig, and D.Johnson,"SEAD:Secure efficient distance vector routing for mobile wireless ad hoc networks,"in *Proc, 8th ACM Int. Conf, Mobicom,2002.*

[7] T.Anantvalee and J. Wu,"A Survey on intrusion detection in mobile ad hoc networks,"in *wireless mobile security.2008.*

[8] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile ad hoc network security,"in *Lecture notes in electrical engineering, vol. 207, 2012.*

[9] D. Johnson and D. Maltz,"Dynamic source routing in *ad hoc* wireless networks," in *Mobile computing,* Norwell, MA:Kluver, 1996.

[10] R. H. Akbani, S. Patel, and D.C. Jinwala,"Dos attacks in mobile ad hoc networks:A Survey," *in Proc, 2nd Int Conf ACCT, Rohtak, 2012.*

K.Sathish, studying B.tech degree in electronics and communication engineering Dr.SJS Paul Memorial college of Engineering & Technology affiliated to Pondicherry university. He had done his schooling at Don Bosco Mat.Hr.Sec.School. He has presented conference at International Conference on Emerging Technology (ICET) and paper presentations in college.

K.Balamurugan, studying B.tech degree in electronics and communication engineering Dr.SJS Paul Memorial college of Engineering & Technology affiliated to Pondicherry university. He had done his schooling at Bon Nehru Hr.Sec.School. He has presented conference at International Conference on Emerging Technology (ICET).

A.Udhayakumar, studying B.tech degree in electronics and communication engineering Dr.SJS Paul Memorial college of Engineering & Technology affiliated to Pondicherry university. He had done his schooling at Calve College Hr.Sec.School. He has presented conference at International Conference on Emerging Technology (ICET).