Manet Network Overhead Is Reduced By Using Elliptic Curve Cryptography

Venkateswarlu Pynam [1], Dr J Anitha [2], Chinaraju Manda [3], Srikanth Kolli

[1] *Assistant Professor, Department of IT,JNTUK-UCEVVizianagaram, India.*
[2] *Associate professor,Malla Reddy engineering collegeIndia*
[3] *Assistant Professor,Department of ECE,JNTUK-UCEV Vizianagaram, India.*
[4] *Assistant Professor, Department of IT,JNTUK-UCEV Vizianagaram, India.*

ABSTRACT: The migration from wired to wireless networks is now a worldwide phenomena. The mobile ad hoc network is a one of the most common and distinctive technologies in today's wireless networks (MANET). Unlike the traditional network design a MANET does not require any additional standardized network's equipment. A single node can be both the sender and the receiver. The nodes communicate directly with one another, despite the fact that they are all in the same field of interaction. Other than that, they are relay on their neighbors to relay for the signals. MANET nodes' self-configuring capabilities make them popular for critical mission applications like military usage or disaster recovery. In this context, it is critical to create successful intrusion and detection methods to safeguard MANET against assaults. We're witnessing the current trend of MANETs being used in industrial applications to decreased hardware cost and the new technological advancements. In order to adapt to this trend and we are all believe that addressing future security flaws is critical. In some cases the EAACK shows enhanced malicious-behavior-detection thresholds while having no effect on system performance, including certain network overhead. We explore and demonstrate the use of mixed cryptographic methods like "The Elliptic curve cryptography (ECC)" is to decrease a network overhead associated with the digital signatures are used in this paper.

Keywords: MANET, EAACK, ECC and Digital Signature

1. INTRODUCTION TO MANET

A mobile ad hoc network (MANET) is just a collection of mobile node's that link directly or indirectly via a wireless communication channel and multimodal wireless connectivity [1]. The ability of wireless networks to enable data transfer between parties while maintaining mobility is one of its most significant advantages. This means that if the distance between two nodes exceeds their individual touch range, they will be unable to communicate. MANET can be used to solve by allowing intermediary actors to relay the data transmissions. There are 2 kinds of MANET networks: single-hop and multi-hop. All nodes inside the same radio range are interact directly with one another in a single-hop network. If the target node is truly outside from radio range, nodes in a multi-hop network are relying on other intermediary nodes to link them. Unlike traditional cellular networks, the MANET has a flexible network design. MANET does not need any specific protocol.

MANETS can be used to collect system data for data mining, and several architectures can be utilized to do so. Given the widespread use of MANET in mission-critical applications such as air pollution control, network security is critical. One of the most important features of these types of applications is that surrounding sensor nodes that monitor the same environmental variable frequently

produce identical results. Because of the geographic similarities between sensor readings, this type of data redundancy has inspired strategies for in-network data aggregation and mining. A wide range of specialized algorithms that including more powerful spatial data mining techniques and more effective routing techniques, may be constructed by estimating the spatial correlation between data gathered by multiple sensors [2]. Despite the fact that most MANET routing methods have limitations, nodes frequently collaborate to relay data. As a result of this assumption, the attackers are left with just one or two compromised nodes capable of having a significant impact on the network. To address this issue and increase the security of MANETs, IDS should be incorporated. An incursion is a series of events that jeopardize a system's security, operation, and integrity. Intrusion detection has evolved into a security tool for detecting those who attempt to get access to and use the computer without an authorization, as well as those who have legitimate access too but misuse it.

An ID watches a device's and users' activities in the system to identify intrusions. Because information systems can have a variety of security weaknesses, building and maintaining a system that is not subject to assaults is both technically difficult and financially costly. They can efficiently track and fight against assaults in pursuit of undesired and unexpected behaviors by monitoring the device and operations of consumers. Network packets are tracked and compared against a database of known hazardous threat signatures or features by IDSs that employ signatures. Other security software detects ransom ware in a similar way. The problem is that there will be a time delay between when a new type of threat is discovered in the wild and when an IDS signature to identify that the threat is developed. During the lag time, your IDS would be unable to detect the most recent threat.

II. LITERATURE SURVEY

In this literature review, I looked at a variety of studies and offered the information that I found most useful.

A. The Wireless Technology for Industrial Wireless Sensor Network:

OCARI is an industrial design for wireless sensor network technology that optimises connections in ad hoc and stable industrial networks. It's made to be utilised in severe environments like power plants and warships. The OCARI is really a wireless networking technology that emphasises mesh architecture and a power-conscious ad-hoc networking protocol to extend network life. Wireless networking will be a major industrial danger in the future years [1]. It provides a number of applications with the purpose of minimising operating costs and boosting industrial performance. WiFi and Bluetooth technologies have been increasingly popular in recent years, infecting both small and large business workplaces. Due to severe surroundings, interference issues and electromagnetic stability, safety, Information Technology security requirements and battery autonomy, these wide public wireless technologies will be constrained in their implementation in the industrial sites. In response to the majority of these industrial requests and challenges, many international organisations such as the Wireless Industrial Networking Alliance, Wireless HART, ZigBee Alliance, and ISA100 have attempted to define and establish industrial wireless infrastructure rules for many technological disciplines [5]. A middleware-oriented WSN should have the purpose of providing consistent services to consumer applications. By adopting a centralised and optimised network management system, it also adds to WSN energy savings. [6].

B. Secure Efficient Distance Vector Routing for mobile wireless ad-hoc networks:

SEAD was developed and evaluated as a modern, stable ad-hoc routing technique for the network that uses distance vector routing. A number of distance vector-based ad-hoc network routing strategies have been developed, although in most cases, a verified atmosphere was required [7]. When building SEAD, we meticulously adapt affordable cryptographic primitives towards each component of the system's operation in order to produce a trustworthy, practical a procedure that is resistant to multiple

disorganized attackers maintaining the wrong route position in any other node, even when the broadcaster's an active attackers or an weak nodes are present. SEAD's system is based on the DSDV ad hoc network routing technique, particularly the DSDV-SQ model, which has already been shown to outperform other DSDV variants in prolonged ad hoc network computations. [8].

C. Detecting Malicious Nodes in Mobile Ad hoc Networks with an Improved Intrusion Detection System:

Several intrusion detection methods have been developed, the bulk of which are strongly connected to routing protocols such as Route guard, Watchdog, and Path rater. There are two aspects to these systems in that one is intrusion detection and other is a response. Each node is equipped with a watchdog that has been trained to detect overhearing. By listening in and reporting to other nodes, each node may identify harmful behavior from its neighbors. On the other hand, if the node that is overhearing and reporting is malicious, it might have a substantial impact on the network output. Ex-Watchdog is an intrusion detection system that uses a single watchdog solution to detect intrusions. Ex-Watchdog fixes Watchdog's fatal flaw, which is that a hostile node can split a network by falsely accusing other nodes of being in danger. Previously employed as a watchdog Agencies are evaluated based on throughput and the overhead, with the certain nodes are being unfriendly type nodes that fraudulently report to the other type of nodes as having problems.

D. To Detecting Forged Acknowledgements in MANETs:

Communication and computer security evaluations have been hampered by the change from physical wire to over-the-air communications. Due to its unique qualities, such as open medium, dynamic topology, and lack of frequent monitoring, MANETs are particularly vulnerable to hostile intruders. Attacks in which no one is participating Packets holding secret information might be intercepted, resulting in a security breach. Active attacks that compromise availability, credibility, authentication, and non-repudiation include injecting packets to erroneous network locations, altering packet contents, deleting packets, and impersonating other nodes [3]. A single mobile node can try to take advantage of other nodes' resources, but it will not share of its own. Greedy or misbehaving nodes are identified by their activities, which are referred to as selfishness or misbehavior [11]. One of the most energy-intensive features of MANET mobile nodes is wireless networking. EAACK2 not only exceeds our previous work in the face of fraudulent acknowledgement messages, but it also maintains the packet headers' security whenever an attack is detected, despite a little increase in computational cost.

III. EXISTING SYSTEM:

Traditional unified monitoring methodologies are no longer viable in MANETs due to their hierarchical architecture and dynamic topology. It's critical to create a MANET-specific intrusion detection device in this situation. Many contemporary MANET IDSs, such as ACK and S-ACK, employ an acknowledgment-based approach. The functioning of the detecting schemes is dependent on the acknowledgement packets. It's critical to make sure that the recognition of packages is real and accurate. They employed a digital signature to overcome this sort of problem in our recommended solution, Enhanced AACK (EAACK). Enhanced Adaptive Acknowledgement has a minor impact on network efficiency, such as network overflow and connection overhead, when used. Every acknowledgement packet must be digitally signed and authenticated before being accepted by an EAACK before being sent out. The "Acknowledgement from start to completion" is what ACK stands for. It is utilized as a part of EAACK's hybrid method when there is no network to reduce the network overhead misbehaviour is observed.

The S-ACK scheme is a more advanced variant of Liu et al TWOACK's scheme. The idea is that every three nodes after that work together to discover problematic nodes. Watchdog's failure to detect

misbehaving nodes in the face of false misbehaviour reports is addressed by the MRA method. False misbehaviour reports can be used by malicious attackers to designate innocent nodes as hazardous. The fundamental aim of the MRA system is to assess if the reported missing packet was received via another way by the destination node. Before entering MRA mode, the source node searches its local knowledge base for another path/route to the destination node. The source node then launches a DSR routing request to locate an alternate path if none is available. MANETs are popular because of their structure, which allows several pathways between two nodes. When implementing the Enhanced Adaptive Acknowledgement technique in MANET, the digital signature has no effect on network or coordination overhead. It can't handle challenges like limited transmission capacity, false misbehaviour reports, and a partial collapse.

IV. PROPOSED SYSTEM:

Many of the current MANET IDS's such as ACK, S-ACK and MRA[4]. When rogue nodes contribute for more than 10% of the total, whatever the case the various digital signatures techniques used in EAACK and It adds to the network's overhead including ACK and S-ACK. The digital signature approach has a larger overhead than the other remaining two techniques, which explains why. We propose and present the use of hybrid asymmetric cryptography, which includes some "Elliptic curve cryptography (ECC)" to further minimize the network cost imposed by digital signatures. The ECC has several advantages over older systems, including having a normal key length (a 160-bit key in the ECC is considered secure), employing arithmetic type operations on such an elliptic curve rather than a finite field, and the ECC's security being dependent on the complexity of an elliptic curve. Discreet logic is a type of logic that is defined as discrete.

V. IMPLEMENTATION:

The most crucial phase in establishing a viable new system and giving consumers confidence that it will work and be useful is implementation. Detailed planning, a review of the current structure and its implementation restrictions, the formulation of changeover procedures, and the assessment of changeover techniques are all part of this stage. ACK, S-ACK, and MRA, two of EAACK's three parts, are both detection based on an acknowledgement techniques. They're all reliant on acknowledgement packets to identify network misbehaviors. As a result, ensuring that all the EAACK acknowledgement packets are legitimate and unhampered with is crucial. Otherwise, if the attackers are clever enough to counterfeit an acknowledgement packet, those three systems will be susceptible. To solve this critical issue, we included a digital signature into our present technique. The EAACK allows every acknowledgement packets to really be a digitally signed until that they are sent to out and validated before that they are accepted, ensuring the IDS's authenticity [8]. The objective is to figure out how to employ digital signatures in MANETs in the most efficient way possible.

Digital signatures are increasingly being used to secure the authentication, legitimacy, MANETs also have non-repudiation. It may be regarded of as a string of data that connects a digital communication to its source or as an electronic version of a signature. "Acknowledgement from start to end" is what the ACK stands for. EAACK's hybrid technique for identifying misbehaving nodes includes it. The S-ACK system is a more sophisticated version of the TWOACK technique proposed by the Liu et al. The idea is that every three nodes after that work together to discover problematic nodes. Following every three nodes along the path, each third node must transmit an S-ACK acknowledgement packet to the first node. Watchdog's fault in detecting errant nodes in the network face of bogus misbehavior reports is addressed by the MRA framework. Malicious attackers can exploit false misbehavior reports to label innocent nodes as dangerous [9].

The network's nodes have the same knowledge folders on a regular basis. To preserve coordination, all nodes will act as cooperation nodes at all times. A message authentication code is a tiny amount of data that is used to verify the authenticity and validity of a communication. Every node will function as an authentication node and store PKI-like information. Many paths can be constructed between a particular source and a particular destination node using multipath routing. To improve the data transmission quality (fault tolerance) or the load balancing, multipath routing is usually advocated. The source network transmits an RREQ message send to all the neighbors within its own listening range throughout the trial. Each neighbor attaches their address to the RREQ letter and distributes it to their neighbors. When a node receives the same sort of RREQ message again, it discards it. A RERR warning is sent to the specific source node if a failures node is to be detected, and that in flat routing protocols such as DSR often indicates a broken connection. When an RREQ message reaches its ultimate destination node, it initiates the delivery of an RREP message to the origin node, reversing the RREQ message's course. It also helps to reduce network overhead to a minimum in most cases. We believe this is related to the hybrid scheme's implementation.

VI. SYSTEM ARCHITECTURE:

The architecture of the system is the process of building a communications network. It's a design framework for things like physical network components, as well as their technical setup, operational standards, procedures, and the file systems utilized in the network and its application.

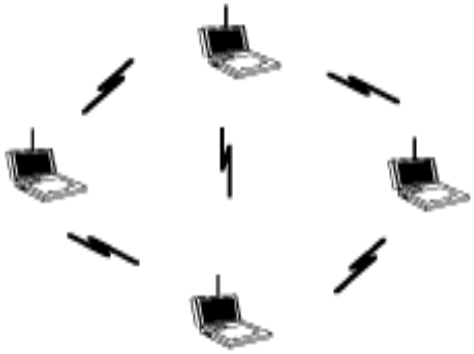

Figure-1: the architecture of a system

6.1 MANET Network Node Creation:

During the network development phase, any node may be formed at both the range described to date and operate on transferring files of information to neighbor nodes processing based on the distance vertical stiffness. Throughout the transmission mechanism, every node in the network is at the same distance from each other. Those same knowledge files can be found in any of the surrounding nodes. To preserve coordination, all nodes will act as cooperation nodes at all times.

6.2 (MAC) Message Authentication Codes and Keys Generation:

A MAC is a short piece of data that may be used to verify the legitimacy of a connection. In this case, each node will act as authentication node and store PKI-like information. The function of a public key cryptography infrastructure is to manage keys and certificates. By allowing the verifiers to detect any changes to the message content, the validity of the Message Authentication Codes protects both the data integrity and the credibility of the message. Cryptographic hash functions and other cryptographic

primitives can be utilized to develop MAC algorithms. Even if one of the cryptographic primitives is subsequently revealed to be vulnerable, the MAC method will ensure that security is preserved.

6.3 Multipath Routing:

It's a routing approach that takes advantage of a network's many paths to provide fault tolerance, lower network overhead, quicker speeds, and improved security, among other things. The multiple paths that have been computed may overlap, be surface disjointed, or have nodes that are disjointed from one another. Multipath routing is used to distribute keys to forwarding nodes, which minimises not just the expense of updating keys in overly complex networks, but also the impact of selective forwarding assaults. Many paths can be constructed between a single source and a single destination node using multipath routing. To increase data transfer efficiency or enable data aggregation, multipath routing is frequently advocated. Alternate route excursion was a sort of multipath routing in classic circuit switched telecommunications networks. Each source and destination node in alternate route routing contains a collection of paths that includes a major path and one or more alternate routes. To improve call blocking while increasing overall network use, alternative route routing was created.

6.4 The Elliptic Curve Cryptography (ECC):

It's a public key cryptography system that encrypts elliptic curves across finite domains using an evolutionary technique. A collection of points (y, x) that fulfil an elliptic curve expression of the type is called an elliptic curve over real numbers of $y^2 = x^3 + ax + b$, where the numbers of a, b, x and y are real values. The elliptic curve question $y^2 = x^3 + ax + b$ that can be put to use construct a group of the expression in $x^3 + ax + b$ has not a recurring variables, Alternatively, if the expression $4a^3 + 27b^2$ is not zero. Elliptic curve classes are additive groups with addition as their primary attribute. An elliptic curve class over all real numbers is formed by the points on the corresponding elliptic curve, as well as a specific point known as the point is at infinity.

ECC is based upon the intractable nature of such issues in mathematics. Because factoring a big integer with two or more broad prime factors is difficult, early public key techniques are safe. The ECDLP, or "elliptic curve discrete logarithm issue," is the assumption that for elliptic curve-based protocols, computing the discrete logarithm for a wild elliptic curve variable with respect to a well-known base point is impractical. When the beginning and product points are supplied, the ECC's security is dependent on the ability to measure a point of multiplication, as well as the inability to measure the multiplicand [10]. The scale of the elliptic curve determines the problem's difficulty. The fundamental benefit of ECC is that it allows for a lower key size, and then which decreases the transmission requirements and storage. As a consequence, an elliptic curve community may provide the same level of security as an RSA-based system with a bigger modulus and, as a result, a larger key. A 256-bit ECC public key, for example, is equally as secure as a 3072-bit RSA public key. It is well-known for its scientific character and intricacy. On a real-number elliptic curve, elliptic curves become points that fulfil the equation $y^2 = x^3 + ax+ b$, here a is to be -1 and b seems to be 1. Elliptic curves feature a variety of mathematical qualities that make them stand out. Because the graph must be symmetric along the x-axis, if (x, y) is a spherical point, so is (x,–y). Any two places on the line with opposing x coordinates will cross the line at a certain third point if you draw a clean line between them. Finally, a straight line drawn from each point on the curve to the cover will intersect the curve at a different place [13].

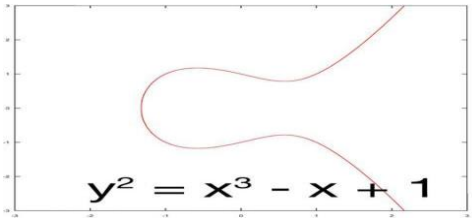

Fig 2: elliptic curves system architecture

In practice, the size of the bit is global key required for ECDSA is roughly two times as big of the elliptic curve cryptography security requirements in bits. At an 80-bit security level, the length of a DSA's public key has been at most 1024-bits; in contrast to an ECDSA's digital certificate is 160-bits long. However, the signature of the size for DSA and ECDSA should be the same: bits, where a bit represents the security level, which is roughly 320 bits for an 80-bit security level. In terms of network overhead, the ECC system still offers a little edge over DSA. This is simple to spot since the signature size of the ECC is significantly less than that of DSA. It's worth noticing that when the number of malicious nodes increases, the RO variances between DSA and ECC algorithms shift. The DSA technique generates more ROs the more bogus nodes there are. This, we believe, is because more number of malicious nodes necessitate additional acknowledgement packets, resulting in a greater digital signature proportion in the overall network overhead. As a result, we believe that ECC is a better digital signature technique for MANETs. The reason for this is that data processing consumes the most battery capacity in MANETs. Although the ECC technique uses more computer resources to check than the DSA system, it still outperforms the DSA approach in terms of accuracy vs battery power and economy.

Symmetric key Size (bits)	RSA & Diffie Hellman Key Size (bits)	Ellipric Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Fig 3: Sizes of keys recommended by (NIST)

ECC can give a degree of security with a key size of 164 bit key then the other systems require a total of 1024 bit key, according to some early researchers work. Because it provides for equivalent encryption while utilising less computing power and battery resources, ECC is becoming an increasingly popular for smartphone applications. RSA has been developing an ECC solution of its own. Many companies, including Motorola, TRW, 3COM, Siemens, Pitney Bowes, Cylink and VeriFone, have been included ECC support in their devices [12].

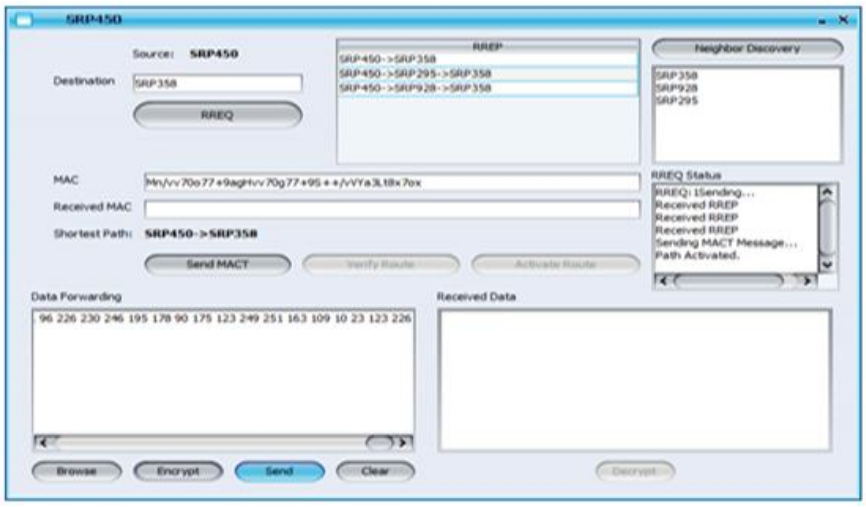

Fig 4: Transmit the encrypted data to the Destination node

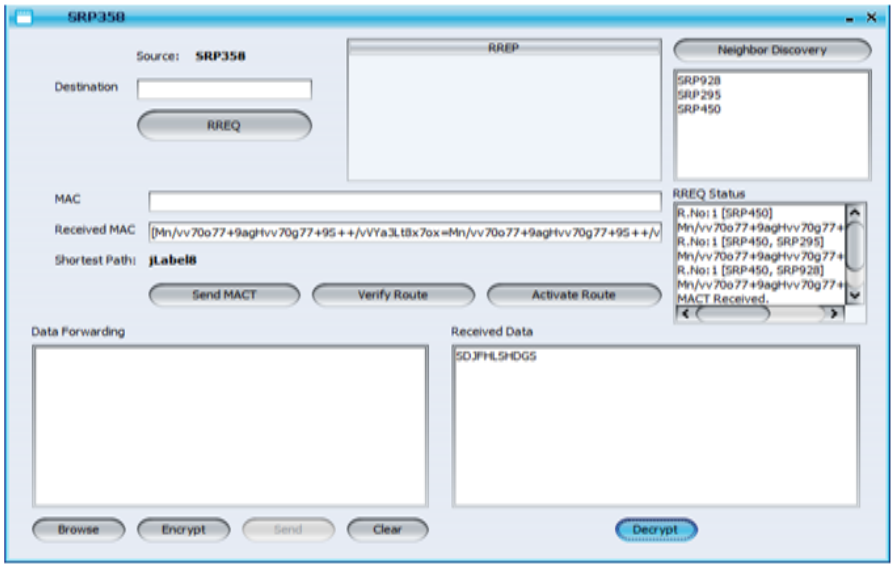

Fig 5: The information is decrypted by the receiver.

Rather of being an ellipse, an elliptic curve is a glide line connecting two axes (oval of shape). The ECC is based on the features of a certain sort of an equation, which are initially taken from a mathematical group generated when the axes are struck in balance. Even if you know the precise point and the impact, determining what number was used to multiply a given point on a curve by generates another point on the same curve is difficult. The equations based on elliptic curves offer a unique feature for cryptography: they are very simple to solve but extremely difficult to change.

6.5 An Elliptic Curves in Practice:

In this part, we look at real-world elliptic curve encryption implementations as well as use data.

A. Bitcoin:

It's a peer-to-peer digital currency that allows anybody to transmit money anonymously without going through a bank. The Bitcoin block chain is a collection of all Bitcoin transactions in chronological order. By linking the blocks starting with the genesis block, the previous block's SHA-256 hash is included in this article's block. The account of a user is generally an ECDSA private key. At the end of a trade, a cryptographic signature of the previous transaction's hash and data about user B's public key are attached to transfer control of bitcoins from user A to user B. User A's public key from the previous block may be used to verify the signature. ECDSA signatures using the secp256k1 curve are used in Bitcoin's cryptographic signatures. A bitcoin address are generated using an ECDSA public key K and the cryptographic hash algorithms like RIPEMD 160 and SHA-256. From any of this HASH160 value, the Bitcoin address is computed as base58, where as base58 is a binary code to the text encoding method.

B. Secure Shell:

Elliptic curve cryptography may be used in three different locations in the SSH protocol. SSH-2 uses a Diffe Hellman key exchange to negotiate session keys. RFC 5656 defines the ephemeral to the Elliptic Curve Diffe Hellman key exchange mechanism used in an SSH. Every server has its own unique host key, which it uses to prove its identity to clients. During the key exchange, the server must send over its host key to the specific client, and the user must verify that the fingerprints of both keys match at the value they registered. The server then authenticates itself by signing a transcript of the key exchange. It's possible that the host key is an ECDSA's public key.

In October 2013, the whole public IPv4 space for SSH host keys, they can serve the signature values and Diffe Hellman values to assess the condition of elliptic curve deployment on server side for the Secure Shell. The compiled a list of each server's key exchange and authentication cypher suites. We used ZMap, a quick Internet-wide port scanner, to look for sites with port 22 open, and then executed a Secure Shell protocol handshake with the addresses that allowed connections on the specified port 22. In order to focus on its elliptic curve real values, our customer just offered elliptic curve cypher suites. As a result, we've observed a wide range of implementations that can produce unexpected responses to our non-standard SSH handshake responses, such as servers that provide RSA or prime order DSA public keys, or servers that provide empty keys.

C. Transport Layer Security:

The Elliptic curves that can be appear in a TLS at various points in the transmission protocol. For TLS, RFC 4492 are the specifies elliptic curve cypher suites. This RFC specifies the use of the elliptic curve Diffe Hellman (ECDH) key exchange mechanism across the whole cypher suite. Either lengthy or ephemeral ECDH keys are possible. The public key included in TLS certificates is used by the server to authenticate itself via an ECDH key exchange. ECDSA or RSA can be used as the public key. In the server and client greeting messages, TLS now offers ECC support for a new set of cypher suites and other different three Extensions. The encryption, key exchange, identity verification, and message validity processes are all supported by the cypher suites. RSA WITH AES 128, ECDHE, TLS, CBC, and SHA, for example, employ ephemeral ECDH for key exchange, authenticated with an RSA key for evidence of identity, the SHA-1 hash a function in an HMAC for secure communication, and AES-128 in CBC mode for encryption.

VII. CONCLUSION

In this study report, EAACK shows higher amount malicious activity of the detection capability while moving data from one point to another in a network while having no influence on network performance, such as network over head. To further minimize the large network overhead imposed by digital signatures, we suggest and put into action of the usage of a hybrid cryptographic techniques known as "Elliptic curve cryptography (ECC)." Finally, we came to the conclusion that the EAACK approach is more suited for use in MANETs. To make our research more useful, we plan to look into a variety of topics in the future: one is to investigate the idea of using a key exchange mechanism to eliminate the need for pre-distributed keys; the other is to test EAACK's performance in a real network environment rather than a software simulation.

VIII. REFERENCE

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

[2]. T. Korkmaz, R. Akbani and G. V. S. Raju, "Mobile Ad hoc Net-work Security," in *Lecture Notes in Electrical Engineering*, 2012, pp. 659–666.

[3]. R. H. Akbani, Patel S, and Jinwala D.C, DoS attacks in mobile ad hoc networks: A survey, in *Proc.* New York: Springer-Verlag, vol. 127. pp. 535–541,2012. *2nd Int. Meeting ACCT,* Rohtak, Haryana, India,

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

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

[6]. A. Bertacchini, D. Dondi, L. Larcher, D. Brunelli, and L. Benini, "Modeling and optimization of a solar energy harvester system for self powered wireless sensor networks," Jul. 2008, *IEEE Trans. Ind. Electron.*, pp. 2759–2766, vol. 55, no. 7.

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

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

[9]. R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, vol. 21, no. 2,pp. 120–126, Feb1983. *Commun. ACM*.

[10]. M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc. Sep 2002, pp. 1–10. ACM Workshop Wireless Security.

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

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

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