How to Cite:
Vinayakan, K., Srinath, M. V., & Adhiselvam, A. (2022). Reinforced securing of data leakage in Mobile Ad hoc Network (MANET) by hybrid mechanism of identity based encryption (IBE). *International Journal of Health Sciences*, *6*(S8), 3622–3635. https://doi.org/10.53730/ijhs.v6nS8.12916

Reinforced securing of data leakage in Mobile Ad hoc Network (MANET) by hybrid mechanism of identity based encryption (IBE)

K. Vinayakan
PG & Research Department of Computer Science, Khadir Mohideen College, Adirampattinam (Affiliated to Bharathidasan University, Tiruchirappalli)
Corresponding author email: k.vinayakan@gmail.com

M. V. Srinath
Department of MCA, Sengamala Thayaar Educational Trust Women's College, Mannargudi (Affiliated to Bharathidasan University, Tiruchirappalli)

A. Adhiselvam
Department of Information Technology, Dr. N.G.P. Arts and Science College, Coimbatore

***Abstract*---**In Mobile Ad hoc Network (MANET), private data leakage that involves user's private keys may become a threat to the computing systems security. It is essential that usual requirement of traditional cryptographic patterns or mechanisms have been performed for enduring several leakage attacks. However, the attacker can track and crack the cryptographic security due to the performance of continuous leakage attacks, which assist in introducing leakage resilience cryptography. But, still there are certain issues such as data loss, data failure system, data affecting and system break that are not yet resolved. As a result, various bounded-leakage models have been created for Identity Based Encryption (IBE) constructions that fail to fulfill their stated security under continuous-leakage assaults. This paper has introduced a hybrid mechanism of security to resolve the above listed issues by focusing in avoiding continuous leakage resilient through modified IBE schemes using Adaptive Chosen Cipher-text Attacks (ACCA) with Elliptical Curve Digital Signature Algorithm (ECDSA).

***Keywords*---**MANET, IBE, SE-AODV, ECDSA, dual ciphertext, security, ACCA-ECDSA, encryption.

Introduction

The MANET is made up of a group of wireless devices that may be moved around. Non-repudiation, integrity, privacy and authentication are some of the security goals that are exhibited by MANET [1]. By keeping a protected channel association between the sender and receiver, these sorts of various objectives can be attained. The system's best route is defined by the quickest method to convey information from one individual to another, mostly determined by the function of a cost [2]. Customary cryptography systems is shown to be secure in a feeble security paradigm, wherein authorized players possess internal secret states like users private keys. The leakage techniques like cold-boot attacks, pattern attacks, selective opening attacks, side-channel attacks and so on, an adversary could discover further data about the internal secret states [3-5]. Conventional encryption methods have lost its requested security, if an opponent acquires a sufficient degree of leakage on internal secret conditions. As a result, for meeting practical security needs of the universe, leakage-resistant cryptographic primitives are critical. However, the most prior leakage-resistant cryptography methods have addressed bounded leakage attacks and continuous leaking is not permitted [6-9]. An exceptional kind of public key encryption is termed as IBE, wherein a device identifier or e-mail address are few string that falls into the category of public key. Thus, the Key Generation Centre (KGC) has act as a reliable third party to generate a private key that matches the string represented as an identity. The recipient's identity is used to encrypt the communication as a public key involves public parameters, without any interaction with the receiver to obtain the public key. A ciphertext is then decrypted with a private key that corresponds to the receiver’s identity.

Subsequently, ECDSA is developed mainly for security characteristics applications, security enhancements and similar like other algorithm that might be vulnerable to security flaws like a random weak source or private key leaking parts [10]. Since, several researchers have enhanced the ECC/ECDSA algorithm's safety by offering countermeasures to numerous threats. However, a balance between efficiency and security is considered while choosing the countermeasures [11]. For symmetric encryption with 80 bits key length, the ECDSA method with 160 bits key length offers the corresponding set [12]. Signature calculation speed offers and employs tiny keys which mainly suitable for limited resource devices [13]. The ECDSA method employs three point multiplication operations are [14]

1. Signature generation
2. Public key creation
3. Signature verification

Various cryptographic methods are employed in MANET for improving the security of routing protocol security. Hashed Message Authentication Code (HMAC) based methods are utilized by secure routing protocol. When the two nodes have been connected and the message authentication cannot be broadcasted, HMAC is used to provide message authentication. When the network routing is secured using time synchronization mechanism like hash chain based methods namely identity based routing and Ariadne as the routing security which designed for general purpose. However, the data transmission needs to be secured

earlier before transmission by generating encryption as well as signature message generation. Therefore, this has been performed by demanding the certificate as identity evidence to the Certificate Authority (CA) for authenticating the received sign certificates from both SN and DN to send and receive the encrypt data. This method is prone to errors and time intensive. The IBC is used for specific characteristics that enable successful authentication in MANETs to overcome several issues. IBE has no storage or communication overhead, making it ideal for implementation in MANETs, unlike the traditional public key infrastructure systems [15].

A novel mechanism is introduced for defending and detecting the continuous leakage of data packets against AODV using ACCA-ECDSA. In particular, AODV protocol performs poorly against several leakage attacks namely cold-boot attacks, pattern attacks, selective opening attacks, side-channel attacks, etc. Initially, secured CCA is implemented in AODV to overwhelming the attacks while comparing with single or awkward attacks. Therefore, the proposed ACCA-ECDSA act as a security encryption mechanism that contributes low overhead computation, transmission and highly efficient against several network attacks as well as continuous leakage attacks.

Literature Review

The literature review discusses a need for efficient security solutions based on various aspects of attacks like networking attacks, as well as continuous leakage present through routing protocol in MANET. This review assists in identifying the properties of an efficient solution and even focus at improving signing key revocation, IBE and enhancing the various efforts that have been made by previous researchers.

Wander et al. have published an energy analysis on the sensor node Mica2dot with Atmel ATmega 128L (8bit) for public key cryptography as Elliptical Curve Cryptography (ECC) and ECDSA. It is discovered that the price of transmission is twice as much as the receiving price. The cost of signature verification in ECDSA is more than the cost of signature creation, but the cost of Rivest Shamir Adlemen (RSA) verification is lower at signatures over ECDSA with a bit-160 key as well as RSA with a bit-1024 key [16].

H.Wang et al found that ECDSA consumes less energy than RSA and also determined ECC/ECDSA is much operational and practical in controlled source devices (WSN) than RSA, since it creates tiny keys and certificates with the same degree of security as RSA. On sensor node MICAz, execution is too carried out for 1024-bit RSA and 160-bit ECC/ECDSA algorithms [17]. The group of concepts for enhancing ECDSA performance by streamlining the algorithm. These concepts comprises of eliminating the reversal in signature creation and signature authentication by means of two points as a replacement for of the shared three curved points, utilizing limited keys and a group of signatures. For the objective of delivering authorization, integration and non-repudiation, the ECDSA method is primarily utilized based on the servers' CA [18].

To allow a node for accessing information, S. B. Othman et al., have suggested an ECDSA threshold based on ID pattern and a trust value with the public key. Furthermore, it is reported that ECDSA data transfer uses extra energy than computing activities in a Wireless Sensor Network (WSN) [19]. To save energy, entire encrypted data collected from all sensor nodes is delivered straight to base station deprived of being decrypted during data transfer which decreases energy usage while extending the life of the network [19].

A.Singh et al use ECDSA for safeguarding the connection amid gateway, nodes and Cluster Head (CH), by bearing in mind different aspects such as memory, protected energy and decreased computation. As the session keys are destroyed after their account, this technique transmits just session keys which save energy. As a result of this procedure, only limited keys are kept in memory and less memory is used. The gateway's public key calculating procedures are carried out with the help of a random number and hash function, which need less computing operations and needs no power [20].

S. Lamba and M. Sharma for the purpose to avoid attacks and suited for constrained-source situations, have proposed a system that uses sporadic authentication in session keys. The revised ECDSA technique proposes generally with two curve points such as public key Q and signature verification point (x; y), using the base point G becoming the private key. As a result, this technique simply uses the s parameter (rather than the r parameter), reducing the r cost. The updated ECDSA method produce higher performance as compared to the unique ECDSA, since it uses fewer point addition, point doubling and PMs [21].

Alwen et al. extended Hash Proof Systems (HPS) in the identity based context and denoted to it as Identity Based Hash Proof Systems (IB-HPS) to combat leakage attacks. They too used it as a starting point for creating CPA safe Leakage-Resistant Identity-Based Encryption (LR-IBE). A common LR-IBE scheme with CPA security is constructed centered on IB-HPS [22].

Chow et al., have suggested three new IB-HPS designs [23]. The common technique may then be used to generate three CPA secure LR-IBE models. In case of ancillary model input, Yuen et al., have proposed an original Continuous LRIBE (CLRIBE) technique that can withstand a more comprehensive kind of leakage [24]. Li et al. proposed a novel LR-IBE scheme centered on Gentry's IBE scheme that could attain CCA security for additionally increasing the security level [25] [26].

The LR-IBE technique with improved performance is devised established on Sun et al. idea, wherein the bits quantity leaked is $\lambda \leq \log q+\omega(\log \kappa)$, as κ is the secret factor and q is underlying group's large prime order [27]. Likewise, the plaintext message and leaking parameter are unrelated. The aforementioned arrangement cannot maintain their stated security in a continuous leakage environment, as it is built using a bounded-leaking paradigm. Thus, Lewko et al. develop the CLR-IBE schemes, and Li et al. could only attain CPA security. CCA security is a powerful and valuable feature, as demonstrated by the basic notion of an encryption system [28] [29]. Zhou et al. lately developed a CLRIBE scheme to

achieve a tall security level, and the method's CCA security is demonstrated in selective identification model [30].

A novel technique of creating a more realistic IBE scheme in the continuous leakage situation deprived of losing CCA security to attain improved performance is presented. On the basis of the difficulty of the q-ABDHE assumption in the standard model, two actual constructions are presented and their security is demonstrated. Simultaneously, it offers a novel technique for developing a realistic IBE system with CCA security and incessant leakage resistance [31]. The recommended protected routing system for MANET, as well as the influence of its parameters on portrayal, like receiving packets throughput, the amount of entire packets dropped, numbers of sending packets is discussed in the preceding sections. The ID centered cryptography method is built and AODV has been updated to include it. The routing protocol protection against malicious nodes by enhancing its capacity to protect itself from unauthorized nodes is suggested by this method. The amount of time it takes to create and verify signatures is also one more factor to be considered [32].

Research Methodology

In this security mechanism, ciphertext encryption cryptography is used in AODV routing packets to identify and prevent rogue nodes as well as leakage attacks that might cause the network to be demolished. However, ECDSA is used as SES algorithm for cryptography which involves key generations like public key as well as private key or secret key. Therefore, ACCA scheme is included in secret key update due to avoidance of any Probability Polynomial Time (PPT). The adversary acquired leakage on secret key from the respective provided ciphertext. Both plaintext encryption and cypher text decoding utilize ACCA-ECDSA method as cryptographic keys. Li et al. demonstrated the building of CAA by presenting a novel LR-IBE arrangement centered on Gentry's IBE arrangement which provide CCA security [26]. This paper has advanced the CAA algorithm by introducing an improved variant as $\prod_N$ and updating the general IBE arrangement using $\prod = (\mathrm{Setup}, \mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$. From the adversary's perspective, the characteristic contained in the ciphertext is random, preventing any leaking of the user's secret key from the corresponding provided ciphertext. This proposed mechanism is considered as a secured encryption for AODV routing protocol in MANET.

Additionally, the Secured Encryption-Ad Hoc on Demand Vector (SE-AODV) is introduced based on encryption secured mechanism in AODV. SE-AODV has offered privacy in MANET for preserving candid exposure of packet drop attacks. During routing data forward, the packet might commence. The presence of leakage attacks or malicious nodes are the reason for the frequent packet drops or leakage. The SE-AODV routing protocol might identify the rogue node or failed connection at the leaking and dropping of packets along the course. For symmetric encryption with a key length of 80 bits, the ECDSA method with a key length of 160 bits offers the equivalent. Since it employs tiny keys and offers calculation speed in the signature which incredibly expedient for devices with limited resources. Furthermore, the recent construction of improved variant as $\prod_N$ is defined with $H(C' \times C' \times C'_T \times C'_T \times \mathbb{Y}_q^* \rightarrow \mathbb{Y}_q^*$ is a hash function for collision resistant and a Key Derivation Function (KDF). While an adequate average min-

entropy is possessed by input, the KDF: $\mathrm{C}_{\mathrm{T}} \longrightarrow \mathbb{Y}_{\mathrm{q}}^{*} \times \mathbb{Y}_{\mathrm{q}}^{*}$ is developed as an average-case robust randomness extractor that could yield a random and constant distribution. Similarly, the element generated by key derivation algorithm is a random value for any intruder. The recent construction illustrated the modification in encryption as Enc_N and decryption as Dec_N whereas the $\prod_{\mathrm{N}}$ is defined as follows

According to the encryption, the $C' \leftarrow Enc_N(id, M)$ is calculated as per given secret key signature message as (r, s) that is considered in term of $r, s, \eta \leftarrow R\mathbb{Y}_p^*$ and computed c_0', c_1', c_2', c_3' and V respectively in equation (1), (2),(3), (4) and (5) as shown below.

$$c_0' = g^s \quad (1)$$
$$c_1' = g_1^r g^{r*id} \quad (2)$$
$$c_2' = e(g,g)^r \quad (3)$$
$$c_3' = e(g,x)^{-r}(g,y)^{-r\eta}M \quad (4)$$
$$V = e(g,x)^{r\mu}(g,y)^r \quad (5)$$

Where,
$\mu = H(c_0', c_1', c_2', c_3', \eta)$

Computing the element c_4' in ciphertext is expressed in equation (6)
$$c_4' = st_1 + st_2 \quad (6)$$

Hence, c_4' is considered as $C' = (c_0', c_1', c_2', c_3', c_4', \eta)$ which has become the signature message M for ciphertext and resulted with ciphertext C'. The verification element is the random value "s" that would be utilized to ensure that ciphertext is effective. "s" could also be chosen arbitrary in the security proof. Similarly, the technique of decryption is derived as $M \leftarrow Dec_N(S_{id}, C')$ whereas the decryption is computed as shown in equation (7) and (8).

$$\omega_1 = e\left(c_1', s_{id,1}\right) {c'}_2^{S_{id,3}} \quad (7)$$
$$\omega_2 = e\left(c_1', s_{id,2}\right) {c'}_2^{S_{id,4}} \quad (8)$$

The ciphertext consistency $C' = (c_0', c_1', c_2', c_3', c_4', \eta)$ is checked $g^{c_4'} = c_0^{t_1'} g^{t_2'}$

Where, $(t_1', t_2') = KDF\left(\omega_1^{\mu}\omega_2\right)$ and $= H(c_0', c_1', c_2', c_3', \eta)$. If the $\mu = H(c_0', c_1', c_2', c_3', \eta)$ is not maintain hold then the results of dummy value is perpendicular or else outcome is represent as $M = c_3'\left(\omega_1\omega_2^{\eta}\right)$ as the plaintext of C'. When executing the algorithm $S_{id}' \leftarrow Update(S_{id}, k_{id})$ which is performed as the subsequent round for decryption operations by setting the secret key as $S_{id}' = \left(s_{id,1}', s_{id,2}', s_{id,3}', s_{id,4}'\right)$. Thus, the ACCA is introduced based on the similar technique but using of improved variant $\prod_{\mathrm{N}}$ form the CCA of IBE scheme. Based on the intruder perspective, any elements present in the ciphertext are random as well as an intruder can't able to accomplish any leakage on the user's private key from the respective given ciphertext.

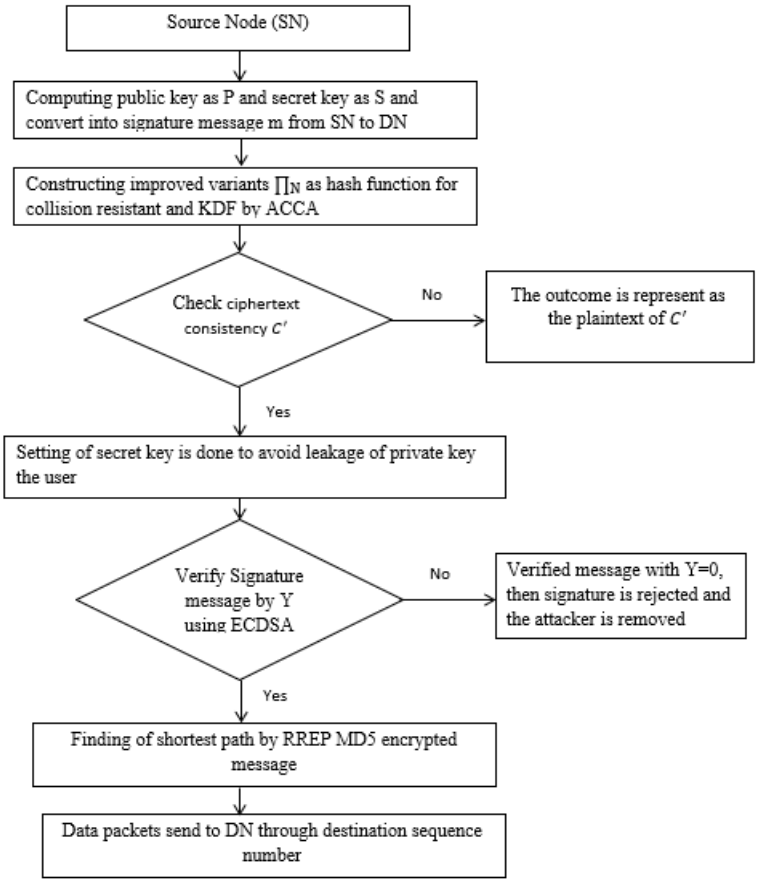

Figure 1 Flow chart for proposed SE-AODV algorithm

The basic concept involved in this proposed ACCA-ECDSA model is encryptions, signatures verification and key management have been concentrated in composing from all nodes are sent to CH. The purpose of the CH is forwarded to the parent aggregators till the secret key reaches the DN. However, it is not assigned for signature verification during the aggregator process, but these processes have been executed only in private key management which is highly capable. Hence, this study has proposed the ACCA-ECDSA model that offers both time consumption and energy efficiency This SE-AODV involves the signature verification process with less time consumption than the signature generation. Moreover, this proposed SE-AODV is suitable for both small as well as large networks. Thus, ACCA-ECDSA model is considered in detail is shown in figure 1 and also involves certain issues that are associated with dual ciphertext cryptography processes in both signature generation and verification.

Algorithm for ACCA-ECDSA

Step 1: Let data packets are send from SN to DN through Route Request (RREQ).

Step 2: The RREQ is generated in term of public key as P and private key as S for encryption by selecting random integers d in interval as [1,n-1] and the key generation is computed P=SG.
Step 3: After key generation, selecting of random integers r for the range of $1 \leq r \leq n-1$ for generating signature is done.
Step 4: Compute signature generation for RREQ and send to all intermediate node as well as DN.
Step 5: The $C' \leftarrow \mathrm{Enc_N(id, M)}$ is calculated as per given private key signature message as Route Reply (RREP) from DN is represented as (r, s) that is considered in term of $r, s, \eta \leftarrow R\mathbb{Y}_p^*$ and computed c_0', c_1', c_2', c_3' and V respectively.
Step 6: Computing the element c_4' in ciphertext as $c_4' = st_1 + st_2$. Hence, c_4' is considered as $C' = (c_0', c_1', c_2', c_3', c_4', \eta)$ which has become the signature message M for ciphertext and resulted with ciphertext C'.
Step 7: Similarly, the technique of decryption is derived as $M \leftarrow Dec_N(S_{id}, C')$ then the ciphertext consistency $C' = (c_0', c_1', c_2', c_3', c_4', \eta)$ is checked $g^{c_4'} = c_0^{t_1'} g^{t_2'}$.
Step 8: When executing the ACCS algorithm $S_{id}' \leftarrow Update(S_{id}, k_{id})$ which is performed as the subsequent round for decryption operations by setting the secret key as $S_{id}' = (s_{id,1}', s_{id,2}', s_{id,3}', s_{id,4}')$.
Step 9: The verification of signature message is done by ECDSA as r and s integers within the interval of [1,n-1].
Step 10: Computing SHA-1(m) as well as converting it as bit string to an integer e and Compute $w = S^{-1} \bmod n$.
Step 11: Similarly computing $u1 = ew \bmod n$ and $u2 = rw \bmod n$. Using those computation Y is calculated as $Y = u1G + u2Q$.
Step 12: If Y=0, then the verified signature is verified as well as rejected and the respective malicious node is removed from route table. Else finding of shortest path by RREP SHA-1 encrypted message.
Step 13: Data packets are send to DN through destination sequence number.

Results and Discussion

The network topology is arranged for this experimental procedure with nodes has been distributed randomly in a rectangular plane area of 1000 m^2. However, the arrangement of the route process is initially progressed by SN for establishing the SE-AODV to intermediate nodes and DN in MANET are iteratively secured using ACCA-ECDSA through RREQ and RREP. This paper focuses to avoid continuous leakage attack and eliminate malicious attacks. The proposed SE-AODV assist to identify a leakage node mentioned in blue color integer and two malicious nodes with red color integer shown in figure 2.

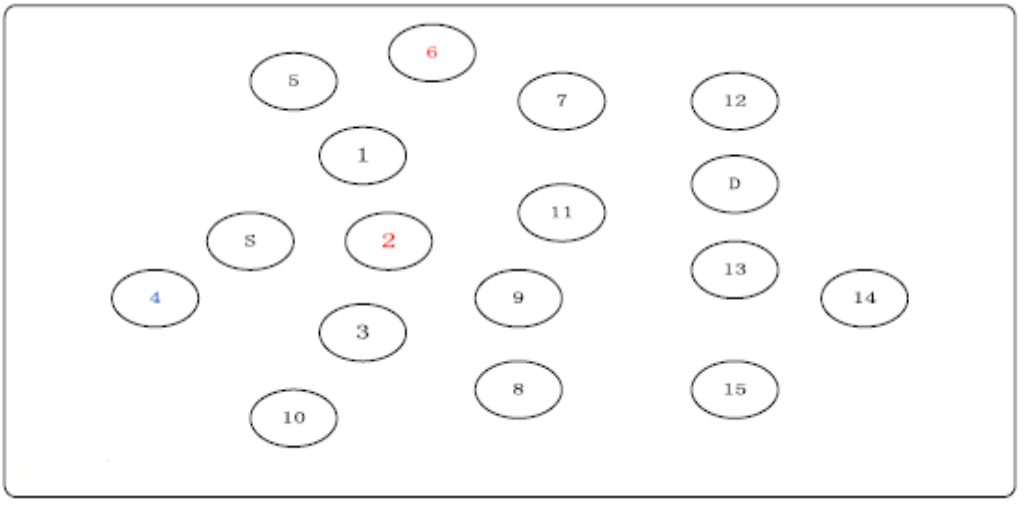

Figure 2 Identification of leakage node and malicious node by SE-AODV protocol

The simulation platform utilized in this paper study is NS3.29 whereas the mobile node numbers range varies from 10 to 50 with the interval of 10 nodes as counts. IEEE 802.11 and Constant Bit Rate (CBR) data stream has adopted in the MAC layer. Moreover, the SE-AODV protocol has been evaluated with several parameters of Quality of Service (QoS) namely throughput, Packet delivery Ratio (PDR), energy consumption and End to End Delay (EED). Therefore, the performance of QoS metrics are compared with IBE scheme AODV (CAA-AODV), digital signature encryption methods like RSA-AODV and ECC-AODV.

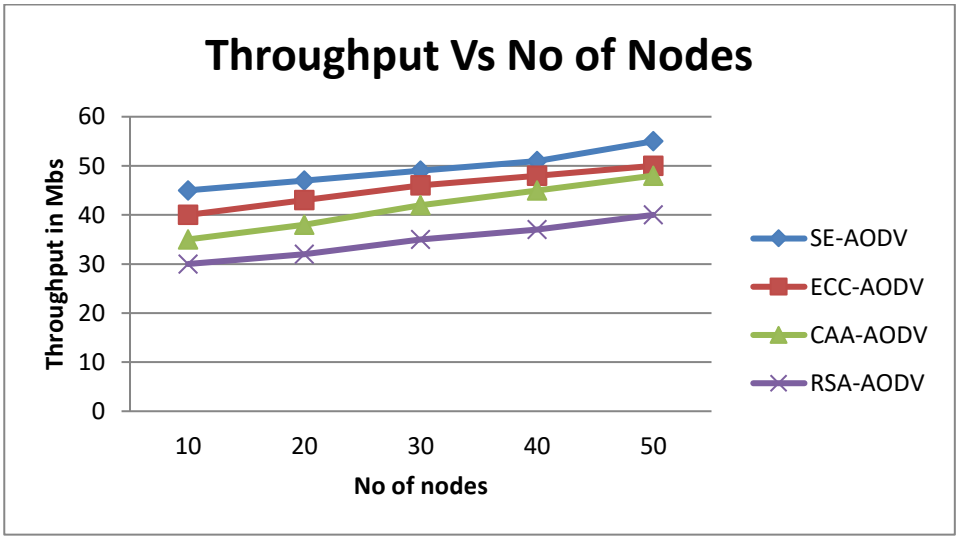

Figure 3 Node Numbers Vs Throughput

The figure 3 has illustrated about the throughput metrics of proposed protocols of SE-AODV with existing IBE and digital signature encryption secured protocols like CAA-AODV, ECC-AODV and RSA-AODV for several nodes from 10 to 50. The throughput of proposed SE-AODV is 45 Mb/s and it gradually increases with

increase of nodes. Moreover, it is comparatively better than existing CAA-AODV, ECC-AODV and RSA-AODV. Hence, the SE-AODV has better throughput result by securing the packet data from intruder. In this research, the simulation result shows that RSA-AODV has accomplished with the least throughput from node 10 to 50.

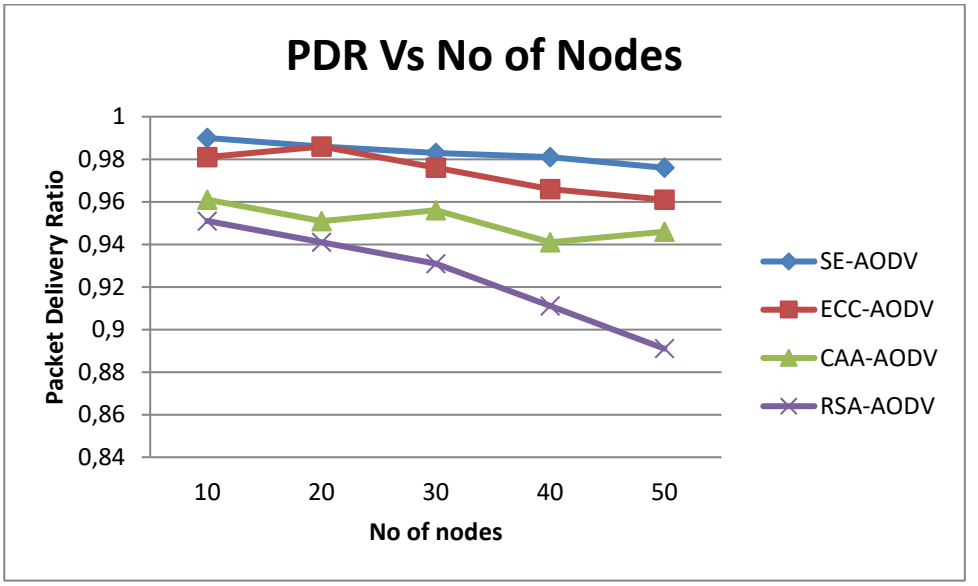

Figure 4 Node Numbers Vs PDR

The figure 4 has illustrated about the PDR metrics of proposed protocols SE-AODV with existing IBE and digital signature encryption secured protocols like CAA-AODV, ECC-AODV and RSA-AODV for several nodes from 10 to 50. The PDR for proposed SE-AODV for node 10 is 0.99 and decrease gradually as the node increases. The PDR of node 20 in ECC-AODV and proposed SE-AODV is similar with the value of 0.986. The comparison illustrate that PDR of proposed SE-AODV is better ECC-AODV CAA-AODV, and RSA-AODV. Similarly, the simulation result shows that and RSA-AODV has obtained the least PDR from node 10 to 50. The3631iguree 5 has illustrated about the EED metric of proposed protocols of SE-AODV with existing IBE and digital signature encryption secured protocols like CAA-AODV, ECC-AODV and RSA-AODV for several nodes from 10 to 50. The time duration of data packet transmission for the proposed SE-AODV get increased with increase of nodes. The time consumed for data transmission in SE-AODV is very less as 31ms in node 10 and 66ms at the node of 50 whereas the compared ECC-AODV CAA-AODV, and RSA-AODV have consumed higher time consumption in data transmission. Moreover, the simulation result shows that RSA-AODV has consumed very high time duration from node 10 to 50.

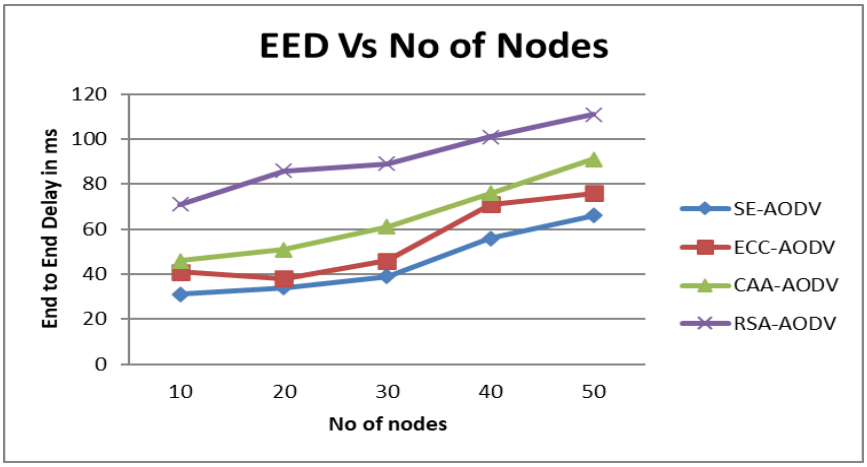

Figure 5 Node Numbers Vs EED

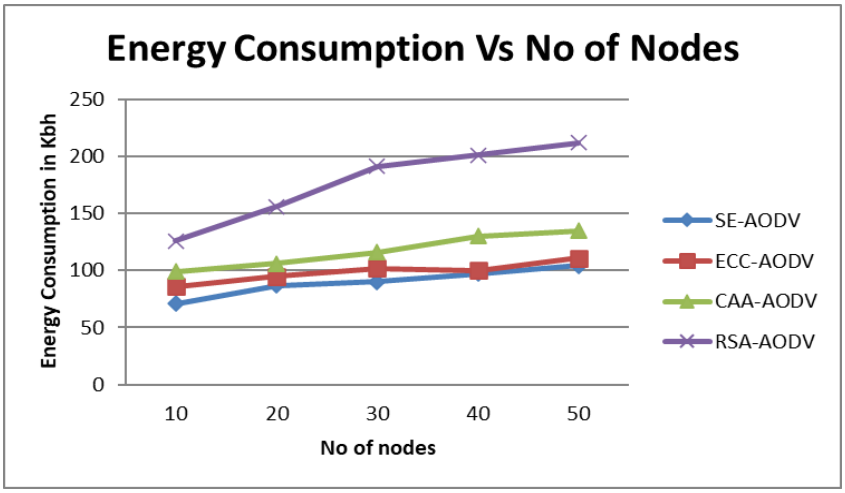

Figure 6 Node Numbers Vs energy consumption

The figure 6 has illustrated about the energy consumption metric of proposed protocols SE-AODV with existing IBE and digital signature encryption secured protocols like CAA-AODV, ECC-AODV and RSA-AODV for several nodes from 10 to 50. The power consumed for data packet transmission in the proposed SE-AODV at node 10 is 71 Kbh which is comparatively lesser than ECC-AODV CAA-AODV, and RSA-AODV. Similarly, the energy consumption is increasing with increase of nodes from 10 to 50 for all proposed and existing routing protocols. The simulation result shows that RSA-AODV has consumed very high energy consumption from node 10 to 50 and the energy consumption for ECC-AODV is slightly closer in the nodes 40 to the proposed SE-AODV.

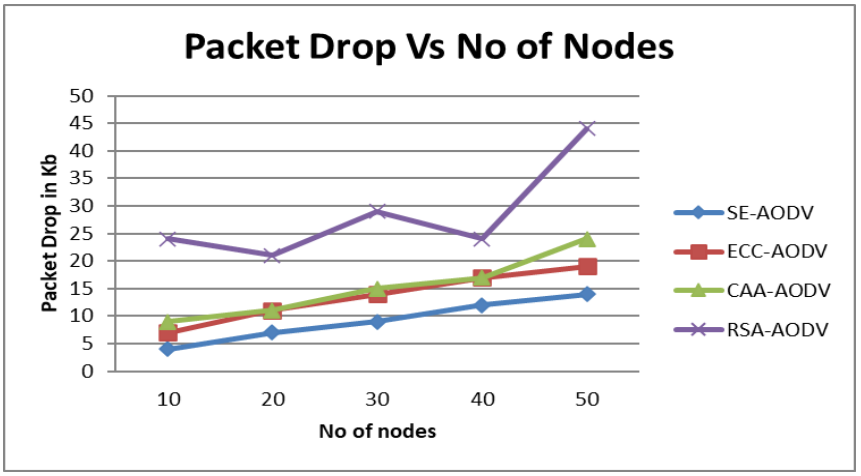

Figure 7 Node Numbers Vs packet drop

The numbers of data packets which have not sent successfully to the destination is measured in figure 7 has illustrated the packet drop metric of proposed SE-AODV with existing IBE and digital signature encryption secured protocols like CAA-AODV, ECC-AODV and RSA-AODV for several nodes from 10 to 50. The packet drop in the proposed SE-AODV for node 10 as 4 and 50 as 14 that is comparatively greater than ECC-AODV CAA-AODV, and RSA-AODV. It has represented the better security of proposed SE-AODV. The results of packet drop shows that increase of node causes increase of packet drops from node 10 to 50. In the case of RSA-AODV, the packet drop is subsequently very high compared with SEAODV.

Conclusion

The scheme of ACCA-ECDSA plays an efficient role in this paper for obtained an improved security in SE-AODV routing protocol in the MANET. However, the role of ACCA-ECDSA may detect and remove the leakage attacks as well as malicious attacks. Therefore, this SE-AODV protocol is continuous leakage resilience and removing the malicious node as well as identifying the shortest route in the route table based on route sequence number. The QoS metric performance of SE-AODV illustrates that improved security protocol assist in enhancing the performance of QoS metrics. The metrics are evaluated with existing IBE scheme based CAA-AODV and also with digital signature encryption methods like ECC-AODV and RSA-AODV. The comparison determines that SE-AODV has better performance than other existing methods. Thus, the proposed dual criphtext cryptography SE-AODV enhances security by providing continuous leakage resilience and eliminating malicious attack in the MANET.

Reference

1. A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, \Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE international conference on pervasive computing and communications. IEEE, 2005, pp. 324-328.

2. A. Singh, A. K. Awasthi, and K. Singh, A key agreement algorithm based on ecdsa for wireless sensor network," in Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, Springer, 2016, pp.143-149.
3. Alwen J, Dodis Y, Naor W, Segev G, Walfish S, Wichs D. Public-key encryption in the bounded-retrieval model. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2010, 113–134
4. Ankur O. Bang, Prabhakar L. Ramteke (2013) MANET: History, Challenges and Applications IJAIEM Volume 2, Issue 9 .pp.249-251.
5. B. Driessen, A. Poschmann, and C. Paar, Comparison of innovative signature algorithms for wsns, in Proceedings of the first ACM conference on Wireless network security. ACM, 2008, pp. 30-35.
6. Chow S S, Dodis Y, Rouselakis Y,Waters B. Practical leakage-resilient identity-based encryption from simple assumptions. In: Proceedings of ACM Conference on Computer and Communications Security. 2010, 152–161
7. Gentry C. Practical identity-based encryption without random oracles, In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2006, 445–464
8. H. Wang and Q. Li, “Efficient implementation of public key cryptosystems on mote sensors (short paper)”, in International Conference on Information and Communications Security, Springer, 2006, pp. 519-528.
9. H. Wang, Z. Wu, and X. Tan, \A new secure authentication scheme based threshold ecdsa for wireless sensor network." in Security and Management, 2006, pp. 129-133.
10. Huang Z G, Liu S L, Mao X P, Chen K F, Li J. Insight of the protection for data security under selective opening attacks. Information Sciences, 2017, 412: 223–241
11. J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, Elliptic curve cryptography in practice," in International Conference on Financial Cryptography and Data Security. Springer, 2014, pp. 157-175.
12. J.-L. Danger, S. Guilley, P. Hoogvorst, C. Murdica, and D. Naccache, A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards," Journal of Cryptographic Engineering, vol. 3, no. 4, pp. 241-265, 2013.
13. Jhaveri R H, Patel N M, Zhong Y B, Sangaiah A K. Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT. IEEEAccess, 2018, 6: 20085–20103
14. Kristin Lauter, (2004), The Advantages of Elliptic Curve Cryptography for Wireless Security, IEEE vol no 20, pp.62-67.
15. Lewko A B, Rouselakis Y, Waters B. Achieving leakage resilience through dual system encryption. In: Proceedings of Theory of Cryptography Conference. 2011, 70–88
16. Li J G, Guo Y Y, Yu Q H, Lu Y, Zhang Y C. Provably secure identity based encryption resilient to post-challenge continuous auxiliary input leakage. Security and Communication Networks, 2016, 9(10): 1016–1024.
17. Li J G, Teng M L, Zhang Y C, Yu Q H., A leakage resilient CCA-secure identity-based encryption scheme, The Computer Journal, 2016, 59(7): 1066–1075
18. Li J G, Yu Q H, Zhang Y C. Identity-based broadcast encryption with

continuous leakage resilience. Information Sciences, 2018, 29(3):177–193
19. S. B. Othman, H. Alzaid, A. Trad, and H. Youssef, An efficient secure data aggregation scheme for wireless sensor networks," in Information, Intelligence, Systems and Applications (IISA), 2013 Fourth International Conference on. IEEE, 2013, pp. 1-4.
20. S. Lamba and M. Sharma, An efficient elliptic curve digital signature algorithm (ecdsa), in Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on IEEE, 2013, pp.179-183.
21. S. Xu, C. Li, F. Li, and S. Zhang, \An improved sliding window algorithm for ECC multiplication," in World Automation Congress (WAC), 2012. IEEE, 2012, pp. 335-338.
22. Sagheer, A. M. & Taher, H. M. Identity Based Cryptography for secure AODV routing protocol. 2012 20th Telecommun. Forum, TELFOR 2012 - Proc. 198–201.
23. Sagheer, A. M. & Taher, H. M. Identity Based Cryptography for secure AODV routing protocol. 2012 20th Telecommun. Forum, TELFOR 2012 - Proc. 198–201 (2012).
24. Sun S F, Gu D W, Huang Z G. Fully secure wicked identity-based encryption against key leakage attacks. The Computer Journal, 2015, 58(10): 2520–2536
25. Sun S F, Gu D W, Liu S L. Efficient chosen ciphertext secure identity based encryption against key leakage attacks. Security and Communication Networks, 2016, 9(11): 1417–1434
26. Sun S F, Gu D W, Liu S L. Efficient leakage-resilient identity-based encryption with CCA security. In: Proceedings of the 6th International Conference on Pairing-Based Cryptography. 2013, 149–167
27. Sun S F, Gu D W, Liu S L. Efficient leakage-resilient identity-based encryption with CCA security. In: Proceedings of the 6th International Conference on Pairing-Based Cryptography. 2013, 149–167
28. T. Cheneau, A. Boudguiga, and M. Laurent, Significantly improved performances of the cryptographically generated addresses thanks to ecc and gpgpu," computers & security, vol. 29, no. 4, pp. 419{431, 2010.
29. Yuen T H, Chow S S, Zhang Y, Yiu S M. Identity-based encryption resilient to continual auxiliary leakage. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2012, 117–134
30. Zhang X S, Tan Y A, Liang C, Li Y Z, Li J, A covert channel over volte via adjusting silence periods. IEEE Access, 2018, 6(1): 9292–9302
31. Zhou Y W, Yang B, Mu Y. Continuous leakage-resilient identity-based encryption without random oracles. The Computer Journal, 2018, 61(4): 586–600
32. Zhou, Y. & Yang, B. Practical continuous leakage-resilient CCA secure identity-based encryption. Front. Comput. Sci. 14, (2020).