Received: June 6, 2018

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Identity Based Key Management Technique for Secure Routing in MANET

Jayanthi Chandrashekar [1]* Arun Manoharan [2]

[1]*Vemana Institute of Technology, India*
[2]*VIT University, Vellore, India*
* Corresponding author's Email: jayansri@yahoo.com

Abstract: Providing a reliable and secure communication in Mobile Adhoc Network (MANET) is a highly challenging and demanding task in recent days. For this purpose, different techniques are developed in the traditional works, but it lacks with the drawbacks of difficult key revocation, reduced security, increased delay, and bandwidth usage. To solve these problems, this paper motives to develop a routing technique, namely, Identity Based Key Management (IBKM) for providing a secure communication in MANET. Here, the group polynomial equation is generated at first for generating a unique ID to each node in the network. Then, the neighboring nodes of the source and destination are identified and registered in the network table. After that, the routing path between these nodes are validated in order to enable a reliable communication. The node pairing is performed and the public key is distributed to the nodes that are successfully paired. Sequentially, the signature of the packet is generated and verified, if both generated and received signature are same, the packet is received; otherwise, the misbehavior node is identified and blocked. To evaluate the results of the proposed mechanism, various performance measures such as malicious node detection probability, average message overhead, Packet Delivery Ratio (PDR), end-to-end delay, throughput, and routing overhead are used. Here, the results are evaluated with respect to various malicious node ratio, speed (m/s), and simulation time (s). Also, the existing Dynamic Source Routing (DSR) and Cooperative Bait Detection Scheme (CBDS) are compared with the proposed mechanism for proving the efficiency. From the results, it is analyzed that the PDR and throughput of the network is increased with the reduced message overhead and delay. Also, the proposed mechanism uses the identity based key management technique, which efficiently detects the malicious nodes in the network.

Keywords: Mobile adhoc network (MANET), Identity based key management (IBKM), Key generation, Security, Public key distribution, Routing path validation, Shamir's secret sharing.

1. Introduction

MOBILE Adhoc Network (MANET) is a self-configured network, which contains an autonomous nodes that can easily join and leave the network at any time[1]. Typically, this network is organized in a decentralized manner, so it does not require any central authority during communication. In this environment, each node is required to trust other node for transmitting the packets, because the mobile nodes are acts like a mediator for routing. The basic design of MANET is presented in Fig 1, where the mobile nodes are connected via a wireless links. The security challenges of MANET [2-4] are as follows:

- Dynamic topology
- Lack of central authority
- Battery constraints
- Insecure environment

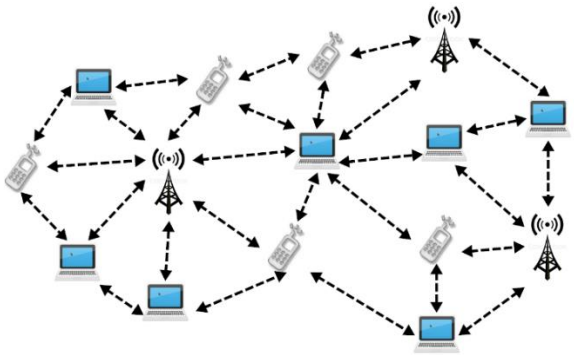

Figure. 1 Architecture of MANET

1.1 Problem description

The routing protocols are mainly required to exchange the routing information between the nodes based on the selected routes [5-7]. When compared to the other wireless infrastructures, the MANET does not have any fixed infrastructure and it has more security threats [8]. For providing a secure communication to MANET, the traditional works develop a various security mechanisms and protocols, but it has some limitations [9-11]:

- Lack of scalability
- Increased computational complexity
- Difficult key revocation
- Increased memory and time consumption
- Key pre-distribution

In order to solve these issues, this paper aims to develop a new security mechanism based on Identity Based Cryptography (IBC) mechanism.

1.2 Objectives

The major objectives of this research work are as follows:

- To securely share the secrets in the network, the Shamir's secret sharing mechanism is implemented.
- To enable a secure and reliable communication in MANET, an Identity Based Key Management (IBKM) technique is proposed
- To avoid congestion and to reduce the overhead, the routing path is selected for pairing the source and destination with the neighboring nodes.

For generating the unique ID to each and every node in the network, the group polynomial equation is used. Based on this ID, the routing path between the source and destination is identified and registered, in which the reliable communication is established by validating the routing path. Moreover, the identity of each node is validated by performing the signature generation and distribution process. Based on the valid signature, the secure communication is established in the network. In order to evaluate the efficacy of this framework, various performance measures such as PDR, malicious node detection probability, average message overhead, end-to-end delay, throughput, and routing overhead are used. Also, some of the existing routing techniques have been considered to prove the superiority of the proposed technique. When compared to these techniques, the proposed IBKM provides the best results by performing the secret generation and key distribution processes.

1.3 Organization

The remaining sectors that present in the paper are structured as follows: the existing routing protocols and key distribution mechanisms used for MANET security are surveyed in Section 2. The clear description about the proposed methodology is presented in Section 3. The experimental results of the proposed key generation and distribution system is evaluated and compared with the traditional mechanism by using different measures in Section 4. Finally, the paper is concluded and the enhancement that will be implemented in the next work are stated in Section 5.

2. Related works

In this segment, various existing frameworks and routing protocols to MANET security are investigated with its advantages and disadvantages.

Rafsanjani and Fatemidokht [12] developed a secure framework, namely, FBee Adhoc based on fuzzy set theory and digital signature. In this paper, various attacks and its impacts were analyzed, which includes forager route related attacks, scout related attacks, and forager route information related attacks. Here, the trust was established between two neighboring nodes for identifying the forager of the packet. Moreover, the fuzzy membership function was utilized in this work in order to improve the security of network. The drawbacks of this work were reduced transmission efficiency, and increased control overhead. Chavan, et al. [13] analyzed the performance of various routing protocols that includes reactive, proactive, and hybrid for secure MANET. The intention of this paper was to identify the most suitable protocol for detecting the black hole attacks in the network. In this investigation, the authors stated that the AODV protocol outperforms the other protocols, due to its increased efficiency. Chang, et al. [14] identified the malicious nodes in MANET by developing a Cooperative Bait Detection Scheme (CBDS) based Dynamic Source Routing (DSR) protocol. This paper aimed to detect and prevent the malicious nodes in MANETs by sensing its address. Here, the feasibility of this technique was analyzed by using a comprehensive routing framework. The drawback of this mechanism was increased computational overhead and reduced efficiency.

Vhora, et al. [15] introduced a Rank Base Data Routing (RBDR) mechanism for identifying the

behavior of the selfish nodes. For this purpose, an Adhoc On-demand Multipath Data Routing (AOMDV) protocol was utilized, which efficiently reduced the packet drop rate. Here, the trusted path was identified for a secure data delivery. However, it has a limitations of reduced delivery ratio and increased delay.Movahedi, et al. [16] developed a trust management framework for estimating the trustworthiness of the nodes in the network. The motive of this work was to detect the harmful attacks in the network based on the trust value with increased detection accuracy. Here, the suggested framework contains the following stages:

- Trust establishment
- Trust level computation
- Knowledge collection

During knowledge collection, the behavior of the nodes was estimated, based on this, the trust of the node was computed. However, this technique has low mobility, and increased computational overhead. Alkhamisi, and Buhari [17] implemented a Trust based AOMDV (TD-AOMDV) protocol for identifying the black hole, gray hole, and flooding attacks in the network. The motive of this work was to enable a reliable and secure communication in MANET with increased throughput. Here, the measured statistics was integrated with the trust values for reducing the overhead. Also, various types of attackers with its routing phases were also discussed in this paper. The major limitations that observed from this paper were, increased energy consumption, and route selection time.

Kaur and Rao[18] implemented a new key management scheme for improving the security of MANET. The stages that involved in this paper were as follows:

- Misbehavior node removal
- Key generation
- Cluster head verification
- Key generation and management

The drawback that observed from this work were, reduced efficiency and energy consumption. Arya and Rajput[19] suggested a Hop Count based Key Selection (HCKS) scheme for minimizing the overhead in MANET. Here, the key pre distribution scheme was utilized to detect various types of attacks at run time. Also, it used a shared secret key for authenticating the end-to-end messages and for establishing the protected route between the source and target nodes. Based on the value of hop count field, the keys were designated from the key table. The drawbacks of this work were increased complexity, and network congestion.

Komboj and Goyal[20] surveyed various key management techniques for enabling a secure communication in MANET. Here, the group key management protocols were classified into three categories that includes centralized, decentralized, and distributed. The processes that involved in key management were as follows:

- Key generation
- Key maintenance
- Key distribution

The major advantage that observed from this work was, it does not required any certification authority. Still, it has a limitation of increased end-to-end delay and time consumption. Sudha, et al[21] introduced a key management paradigm for enabling a secure broadcast in MANET. For this purpose, the group encryption was extracted, which reduced both communication cost and computation overhead of the network. In this mechanism, a Certificate Authority (CA) created and validated the public key during message transmission. The techniques that were used for distributing the public keys for increasing the level of security. It utilized the following techniques:

- Public key certificates
- Key separation
- Controlling use of symmetric keys
- Authentication trees

The benefit of this work was, it reduced the complexity and reduced the amount of time required for encryption. However, the level of security should be improved by implementing an advanced mechanisms.Park and Park[22] developed a key revocation scheme for identifying the misbehavior of the nodes in MANET. For this purpose, the authors analyzed the fundamental security services, and non-manipulation. Also, the secret sharing scheme was utilized in order to efficiency of the network. Here, the multimedia data was shared with privacy key generation and revocation. However, the detection efficiency of this scheme was not in a satisfied level.Renugadevi and Mala[23] implemented a Ternary Tree based Group ECDH (TGECDH) protocol for increasing the computation and communication efficiency of the network. Here, the underlay approach was used to simultaneously access the band at both Secondary Users (SUs) and

Primary Users (PUs). Moreover, this scheme comprises the following stages:

- Preprocess
- Merge

In this analysis, the performance of this key distribution mechanism was fully depends on the structure of the key. The advantage that observed from this work was, it provided a secure communication between the users, so it was highly suitable for the dynamic groups. Still, it has the disadvantage of increased latency and reduced throughput. Kalambe and Apte [24] surveyed various security solutions against different types of attacks in MANET. Here, the behavior of all the nodes in the network were analyzed based on the principles of integrity, confidentiality, and authenticity. Moreover, different types of layer attacks were discussed. Verma, et al. [25] surveyed various QoS based routing protocol for improving the security of MANET. Here, a trusted infrastructure was formatted using AODV protocol for preventing the network against attacks. Also, the major security requirements were discussed for analyzing the security level of MANET. In this work, it was stated that the AODV protocol offered an efficient route discovery compared than the other protocols. Dhivya, and Kavitha [26] used three different techniques such as Time To Live (TTL) mechanism, piggy backing, and prefetching for maintaining the sustainability of MANET. Here, the Distributed Cache Invalidation Method (DCIM) was utilized to reduce the cost of cache data. The limitation that observed from this paper was, it required to enable an error free communication by improving the security. Mafra, et al. [27] recommended a cryptographic based fault tolerance mechanism for detecting both faulty and malicious nodes in MANET. The motive of this mechanism was to maintain the reliability and security of the network with increased attack detection rate. Bhatia and Verma [28] surveyed various security issues for providing a better solution to secure routing. Here, a broad analysis about the security issues, and vulnerabilities was provided. But, it required to optimize the security solution by considering the Quality of Service (QoS), which was the major limitation of this paper.

From this investigation, it was analyzed that the existing techniques have both advantages and disadvantages, but it mainly lacks with the disadvantages of increased overhead, reduced delivery rate, and inefficient communication. Thus, this paper aims to develop an identity based key distribution mechanism for MANET security.

3. Proposed method

In this sector, the clear description about the proposed methodology is provided. The intention of this paper is to ensure the reliable communication in MANET by providing a secure key generation and distribution. For this purpose, an Identity Base Key Management (IBKM) technique is proposed in this paper. Here, the security level of the network is increased by implementing an efficient key generation, distribution, and verification processes. Fig. 2 shows the flow of the proposed IBKM based secure MANET routing mechanisms, which includes the following stages:

- Node registration
- Routing path validation
- Key generation, distribution, and validation
- Signature generation and verification

Initially, the network is formed with the mobile nodes, and group polynomial equation is generated for generating the unique ID to every node in the network. Then, the neighboring nodes of the source and destination are identified and registered by using the ID. After that, routing path between the

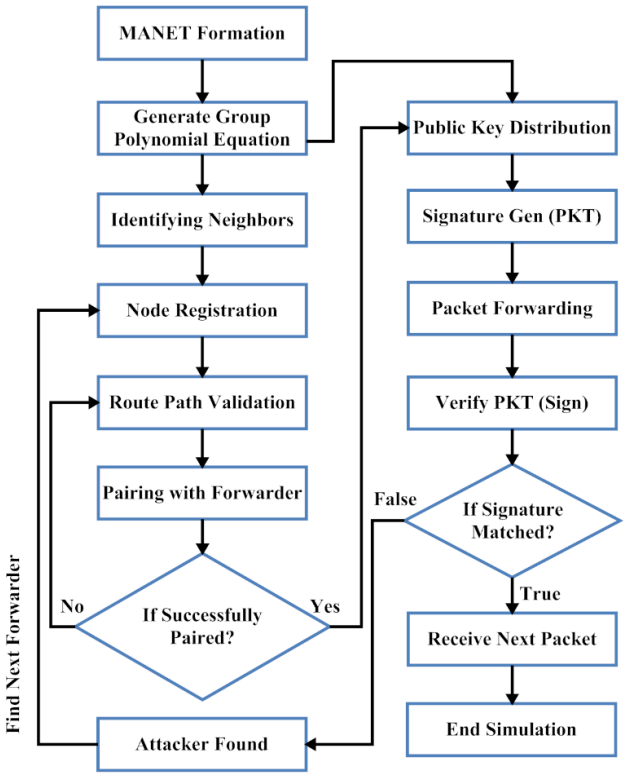

Figure. 2 Flow of the proposed system

source and destination is validation in order to enable a reliable and secure communication. Consequently, the forwarding nodes are paired and verified, if both are matched, the public key is distributed to all the nodes in the network. Otherwise, the next forwarder is identified with node registration process. Then, the signature generation and distribution processes are performed to verify the identity of the nodes. If the signature is valid and matched, the next packet is received and, the secure communication is enabled.

3.1 Node registration

Initially, the polynomial equation is generated to create the unique ID for each and every node. Based on this ID, the neighboring nodes of both source and destination are identified in order to ensure the valid routing path. Let, *AF(s)* is a finite set, and *X(a, b)* is the symmetric polynomial of degree d with the coefficients in *AF(s)*;

$$X(a,b) = X(b,a) \tag{1}$$

Where, node n_i receives the polynomial $q_i(a) = P(a,i)$, node n_j receives the polynomial $q_j(a) = P(a,j)$, and the common key between i and j is computed by $P(i,j) = P(j,i)$. Then, the neighboring nodes are registered in the network table based on an authentication process. If the normal node requests to register, the admin of the network provides an access for a certain amount of time. Moreover, a mobile node should send a registration request to register with its home network.

3.2 Route path validation

After registering the node, the routing path is validated in order to ensure the reliable communication. Routing is an important criterion in network security, which maintains the stability of the link by avoiding the link and path failure. During this process, the path from source to destination must have the least hop distance, if there is any failure in the primary path, the secondary path is selected by authentication. The routing path is validated by checking the link stability of the transmission route.

3.3 Key generation, distribution, and verification

After validating the routing path, the key is generated based on the unique ID of the node. During this process, the public and private key pair is used for authenticating the node. The identity based key management enables an end to end authentication between the source and destination nodes. It ensures the identity of the node by authenticating the mobile nodes in the network. Here, the communicating nodes creates the secret at both side without additional key exchange. In this paper, an IBKM technique is proposed for generating and distributing the keys in the network, which is clearly described in Algorithm I. In which, a random co-prime number is selected at first, then the total number of nodes in the region *n* and its threshold *k* are obtained. Based on this, the random secret SK_i is generated, then each node in the network distributes a secret between the other nodes. After that, the shared key of the participant nodes are computed by using the generated matrix, and rank of the shared vector. Subsequently, the nodes in the set uses the polynomial production protocol for generating the random secret key with the threshold. Finally, the shared secret is recovered by using the lagrangian interpolation of the nodes.

Algorithm I – Identity Based Key Management

Step 1: Select a random co-prime number cP;

Step 2: Get the total number of nodes in the region n and k threshold $k \in cP$*;*

Step 3: Generate the random secret $SK_i \in cP, 1 \leq i \leq k$*, such that* SK_i *is the* i^{th} *element in the secret key pool S;*

Step 4: Each n node P_i *distributes a secret called* $\delta_{i,i} \in [1,t]$ *between the entire nodes, where t – 1 is the degree of the polynomial secret sharing;*

Step 5: Each node includes its shares of δ_i *as one. As a outcome, every node has a own share on t – 1 degree polynomial* $g(x)$ *with a constant term* $\delta = \sum \delta_i$*;*

Step 6: Compute the shared key of participant nodes based on the following function:

$$f(s) = f\left(\sum_{i=1}^{k} s_i\, e_i\right) = \sum_{i=1}^{k} s_i f(e_i)$$

$$= sG = (t_1, t_2, \ldots . t_n)$$

//Where, G is $k \times n$ *generator matrix, the rank of G is k, and* $(t_1, t_2, \ldots t_n) = T$ *defines the share vector;*

Step 7: Distribute the keys to n nodes such that i^{th} participant gets t_i^{th} key for $1 \leq i \leq n$;

Step 8: The nodes in the set cP use the polynomial production protocol for generating the random secret key β_i shared with threshold$t \in min[t_i, t_{i+1} \dots t_m]$;

Step 9: Nodes n_i andβ_i shares the final key set;

$cP = cP - \{n\} for\ level\ Lm$;

Based on cP, the constant of $i \in [1, m-1], \alpha_{i+1} = \alpha_i + \beta_i$ is calculated; //Where, $\{\alpha_1, \alpha_2, \dots \alpha_m\}$ remains the shared key of α_m;

Step 10: If a set Δ_i' of at least t_i' nodes cooperates by using the lagrangian interpolation, the secret key is recovered as follows:

$Secret_i = \sum_{j \in \Delta_j'} (\gamma_i \times \varphi_j)$ *is termed as* α_1;

//Where, $\gamma_j = \int_{j \in \Delta, j \neq 1} \frac{j}{j-1}$ $for\ all\ i \in \Delta$;

$\varphi_j = \sum_{i=\Delta} (\gamma_j \times g_i(j))$ *is used for calculating the new shared key;*

$\alpha_{i+1} = \alpha_i + \beta_i \bmod q\ for\ i = (m-1)\ from\ that\ \alpha_i$ *is recovered;*

3.4 Signature generation and verification

Signature generation is a mechanism that is mainly used to offer an increased protection to the data. Here, the shamir's secret sharing mechanism is implemented to generate and verify the signature of the packet. In this mechanism, the signature of the original message is verified, and also it verifies the malicious nodes. The nodes are authenticated and the integrity of routing is ensured by using the signatures. The main reason of signature generation and verification is, it offers packet integrity. This technique requires one way hash function for the positive integer *x*, which is represented as follows:

$$h: \{0,1\}^* \rightarrow \{0,1\}^x \quad (2)$$

Where, $\{0,1\}^x$ indicates the bit strings and $\{0,1\}^*$ is the set of all bit strings. During signature generation, the source node performs the following functions:

Algorithm II – Signature Generation and Verification

Step 1: It selects the random number a, $1 \leq a \leq n-1$;

Step 2: Then, the generation coefficient of the packet of

$\omega = a^2 \bmod n$ *is computed;*

Step 3: Also, $e = (e_1, e_2, \dots e_k) = h(m||w)$ *is computed for each* $e_k \in \{0,1\}$*;//Where, e – encryption key for k number of packets, m – message;*

Step 4: The signature shares $= a \cdot \Pi_{j=1}^{k} s_j^{e_j} \bmod n$*; //Where,*$s_j$ *– shared key of the j^{th} node and n – number of nodes;*

Step 5: Lastly, the signature of the source node is defined for m is (e,s).

//The signature verification is performed as follows:

Step 1: Obtain the authentic public key of the source,$(v_1, v_2, \dots v_k)$ *and n;*

Step 2: Compute the reconstructed coefficient value of $u = s^2 \cdot \Pi_{j=1}^{k} v_j^{e_j} \bmod n$;

Step 3: Estimate the value of $d = h(m||u)$*; //Where, d – decrypted packet;*

Step 4: Validate and accept the signature if $e = d$;

The major advantages of this work were as follows:

- Reduced overhead
- Increased delivery ratio
- Efficient communication
- Minimized delay
- Complex key generation

4. Performance analysis

In this sector, the performance results of the traditional and proposed IBKM mechanisms are analyzed by using the measures of malicious node detection probability, Packet Delivery Ratio (PDR), average message overhead, end-to-end delay,

Table 1. Experimental settings

Parameter	Value
Application traffic	CBR
Transmission interval	250m
Radio range	250m
Packet size	512 bytes
Channel data rate	11 Mbps
Pause time	0s
Maximum speed	10 m/s
Simulation time	100 s
Number of nodes	100
Malicious nodes	0% to 40%
Threshold	Dynamic threshold
Area	1500m ×1500m
Malicious agent	Hacker agent (AODV)

throughput, and routing overhead. The experimental setting of this paper is illustrated in Table 1.

4.1 Malicious node detection

Fig. 3 estimates the probability of malicious node detection rate is analyzed with respect to the ratio of malicious nodes in the network. This probability is estimated for both existing [14] Dynamic Source Routing (DSR), Cooperative Bait Detection Scheme (CBDS) and proposed IBKM techniques. In this analysis, the total number of malicious nodes are represented in the x-axis, in which the detection probability of the existing and proposed techniques are calculated and represented in y-axis. From this, it is observed that the proposed IBKM has the increased detection probability, when compared to the other techniques.

4.2 Packet delivery ratio

Here, the PDR measure is calculated based on the number of packets sent by the source and the number of packets received by the destination. It is estimated as shown in below:

$$PDR = \frac{1}{n}\sum_{i=1}^{n}\frac{PD_i}{PS_i} \quad (3)$$

Where, PD_i indicates the total number of packets that are successfully received by the destination with the i^{th} application, and PS_i defines the number of packets that are actually sent by the source. Fig. 4 shows the PDR of the existing DSR, CBDS, and proposed IBKM techniques with respect to the ratio of malicious nodes in the network. Also, the PDR is estimated with respect to varying node speed (m/s) as shown in Fig. 5. Fig. 6 compared the existing[29], [30] RTA, SHEATH and proposed IBKM techniques with respect to varying simulation time (ms). In this evaluation, it is stated that the proposed PDR of the proposed IBKM is increased, when compared to the other techniques.

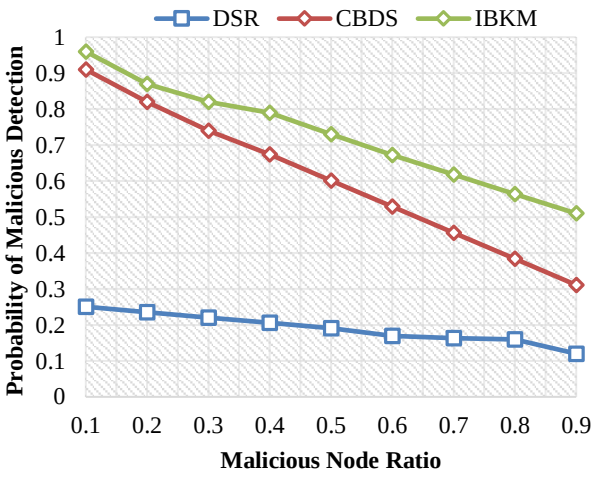

Figure. 3 Malicious node detection probability

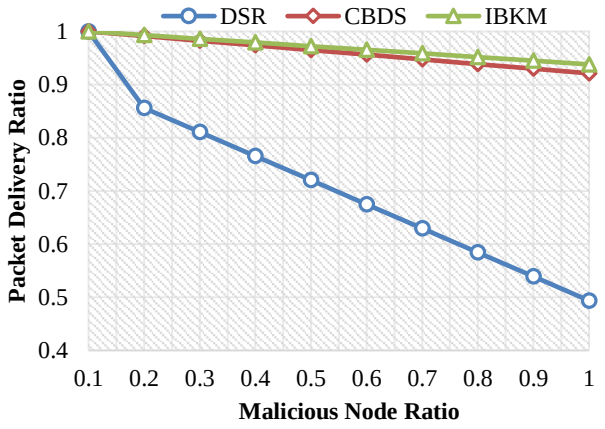

Figure. 4 Packet delivery ratio

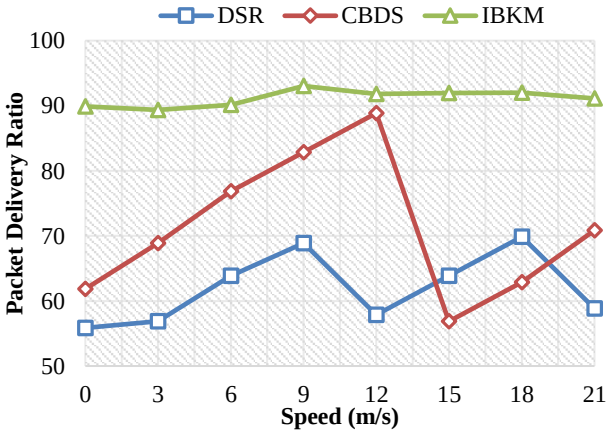

Figure. 5 Packet delivery ratio Vs Speed

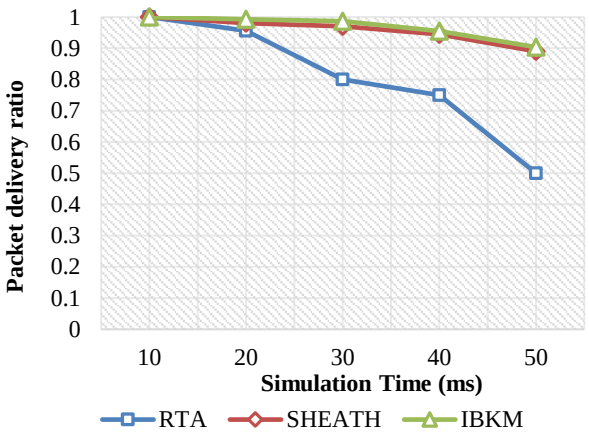

Figure. 6 Packet delivery ratio Vs Simulation time

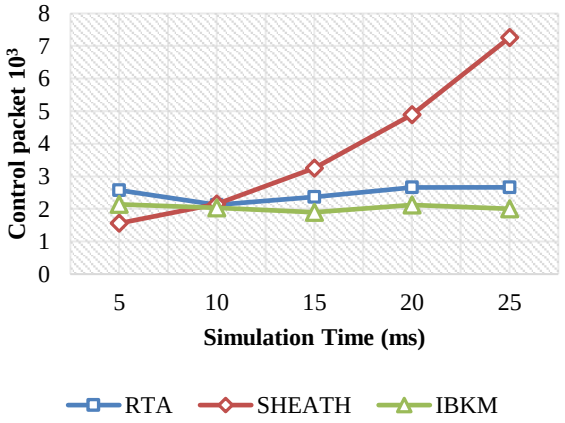

Figure. 8 Average message overhead

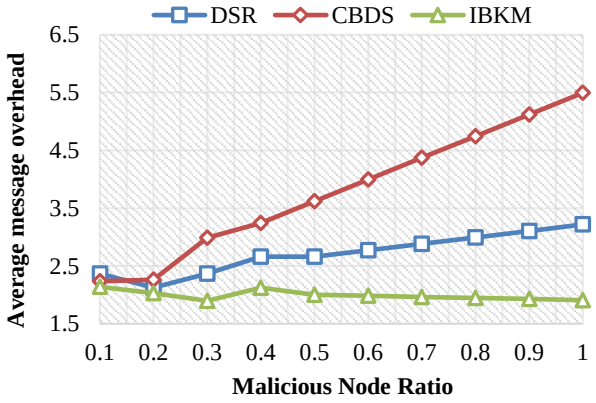

Figure. 7 Average message overhead

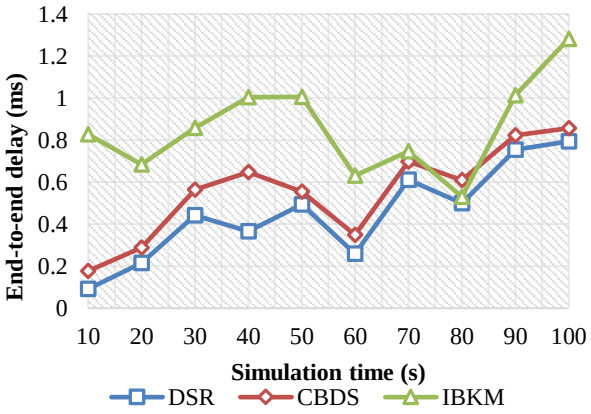

Figure. 9 End-to-end delay

4.3 Average message overhead

The average message overhead is defined as the number of additional messages used to attain the acceptance rate of improvement. Fig. 7 illustrates the average message overhead of existing DSR, CBDS, and proposed IBKM techniques with respect to malicious node ratio. Similarly, Fig 7 compares the average message overhead of existing RTA, SHEATH and proposed IBKM techniques. Here, the control packet contains the user data and payload information such as error detection code, sequence information, and destination network address. In this evaluation, the average message overhead is compared with the existing techniques based on the number of transferred control packets and simulation time. Based on this, the average message overhead occurred between the source and destination nodes is calculated. When compared to the other techniques, the proposed IBKM has the reduced message overhead.

4.4 End-to-end delay

It is the total amount of time occupied by the packet to range the destination from the source. Fig. 9 shows the end-to-end delay of the existing DSR, CBDS, and proposed IBKM techniques with respect to malicious node ratio. Then, Fig. 10 compares the delay of existing RTA, SHEATH and proposed IBKM techniques with respect to varying simulation time (ms). It is calculated as follows:

$$E = \frac{1}{n}\sum_{i=1}^{n}\frac{d_i}{PD_i} \quad (4)$$

Where, the delayed packet acknowledged by the target is indicated as d_i and the total number of packets established by the destination is indicated as PD_i. From this analysis, it is observed that the proposed IBKM has the reduced delay, when compared to the other techniques.

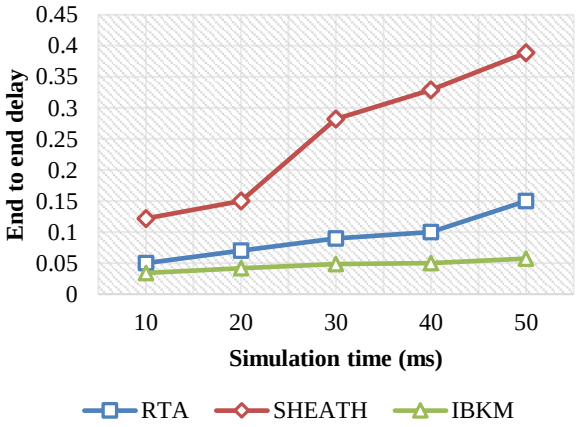

Figure. 10 End-to-end delay

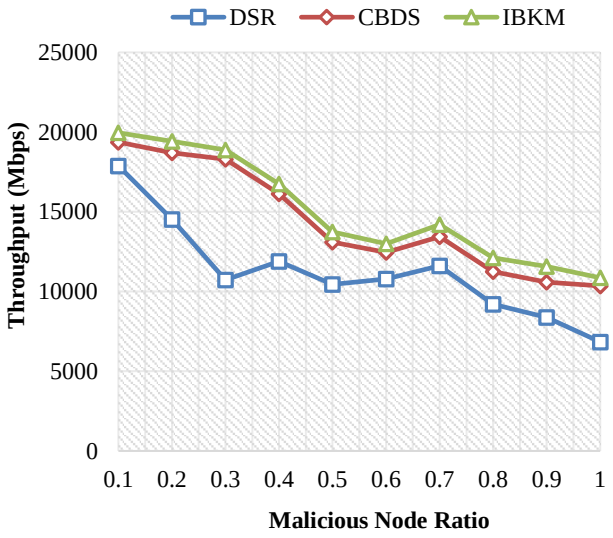

Figure. 11 Throughput

4.5 Throughput

Throughput is the ratio of the total amount received data by the destination, and the amount of time taken by the destination to get the final packet. It is calculate d as follows:

$$TH = \frac{1}{n}\sum_{i=1}^{n}\frac{TD_i}{T_i} \quad (5)$$

Where, TH indicates the throughput, TD_i is the amount of data received by the destination, and T_i is the time. Fig. 11 shows the throughput of existing DSR, CBDS, and proposed IBKM techniques with respect to malicious node ratio. In this analysis, it is stated that the proposed IBKM provides an increased throughput, when compared to the other techniques.

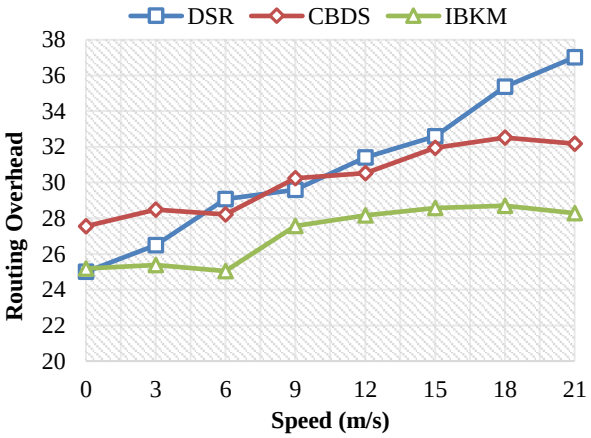

Figure. 12 Routing overhead

4.6 Routing overhead

It is defined as the ratio of the routing related control packet transmission by the amount of transmission. It is estimated as follows:

$$RO = \frac{1}{n}\sum_{i=1}^{n}\frac{CK_i}{DK_i} \quad (6)$$

Where, RO is the routing overhead, CK_i is the total number of control packets transmitted, and DK_i indicates the number of transmitted data packets. Fig. 12 shows the routing overhead of existing DSR, CBDS, and proposed IBKM techniques with respect to varying speed (m/s). Here, it is proved that the proposed IBKM has the reduced routing overhead, when compared to the other techniques.

5. Conclusion and future work

In this work, an efficient IBKM technique is proposed for ensuring a secured communication in MANET. The contributions that have been mainly focused on this work are increased security, reduced delay and communication overhead. For this reason, an efficient secret and key generation mechanisms are implemented, which intends to establish a secure communication in MANET. Here, the group polynomial equation is generated for creating the unique ID to each node in the network. Then, the neighboring nodes between the source and destination are identified by using this ID, then each node that participate in the communication registers into the network table. After that, the routing path is validated for ensuring the reliable link between the sender and target. Here, the node pairing is performed for pairing with the forwarder node, if the nodes are successfully paired, the public key is distributed, and the signature is generated for forwarding the packet. If the signature is valid, the packet is received and the communication is

proceeded. Otherwise, the attacker is detected and the next forwarder is identified for communication. During experiments, the results of existing and proposed routing mechanisms are validated by using the measures of PDR, malicious node detection probability, end-to-end delay, throughput, routing overhead, and average message overhead. In this evaluation, it is proved that the proposed IBKM provides the improved results compared than the other techniques by implementing an efficient secret and key generation mechanisms.

In future, this work can be enhanced by implementing the soft computing techniques for analyzing the behavior of the nodes in the network.

References

[1] K. Dhanalakshmi, B. Kannapiran, and A. Divya, "Enhancing manet security using hybrid techniques in key generation mechanism", In: *Proc. of the 2014 International Conference on Electronics and Communication Systems*, pp. 1-5, 2014.

[2] A. Kumar, K. Gopal, and A. Aggarwal, "Design and Analysis of Lightweight Trust Mechanism for Secret Data using Lightweight Cryptographic Primitives in MANETs", *IJ Network Security*, Vol. 18, pp. 1-18, 2016.

[3] P. Memarmoshrefi, R. Seibel, and D. Hogrefe, "Autonomous Ant-based Public Key Authentication Mechanism for Mobile Ad-hoc Networks", *Mobile Networks and Applications*, Vol. 21, pp. 149-160, 2016.

[4] A. Dorri, S.R. Kamel, and E. Kheirkhah, "Security challenges in mobile ad hoc networks: A survey", *arXiv preprint arXiv:1503.03233*, 2015.

[5] H. Kaur, V. Sahni, and M. Bala, "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review", N*etwork*, Vol. 4, pp. 498-500, 2013.

[6] P. Gulia and S. Sihag, "Review and Analysis of the Security Issues in MANET", *International Journal of Computer Applications*, Vol. 75, pp. 23-26, 2013.

[7] V. Goyal and G. Arora, "Review Paper on Security Issues in Mobile Adhoc Networks", *Engineering and Science*, Vol. 2, pp. 203-207, 2017.

[8] A.K. Maurya, D. Singh, A. Kumar, and R. Maurya, "Random waypoint mobility model based performance estimation of On-Demand routing protocols in MANET for CBR applications", In: *Proc. of the 2014 International Conference on Computing for Sustainable Global Development*, pp. 835-839, 2014.

[9] S.K. Sharma, R. Kumar, A. Gangwar, and K. Pakhre, "Routing protocols and security issues in MANET: A survey", *International Journal of Emerging Technology and Advanced Engineering*, Vol. 4, pp. 918-924, 2014.

[10] S. B. Sharma and N. Chauhan, "Security issues and their solutions in MANET", In: *Proc. of the 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management*, pp. 289-294, 2015.

[11] P. Singh and G. Singh, "Security issues and link expiration in secure routing protocols in MANET: a review", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 3, pp. 559-565, 2014.

[12] M. K. Rafsanjani and H. Fatemidokht, "FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs", *AEU-International Journal of Electronics and Communications*, Vol. 69, pp. 1613-1621, 2015.

[13] A. Chavan, D. Kurule, and P. Dere, "Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack", *Procedia Computer Science*, Vol. 79, pp. 835-844, 2016.

[14] J-M. Chang, P-C. Tsou, I. Woungang, H-C. Chao, and C-F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach", *IEEE Systems Journal*, Vol. 9, pp. 65-75, 2015.

[15] S. Vhora, R. Patel, and N. Patel, "Rank Base Data Routing (RBDR) scheme using AOMDV: A proposed scheme for packet drop attack detection and prevention in MANET", In: *Proc. of the 2015 IEEE International Conference on Electrical, Computer and Communication Technologies*, pp. 1-5, 2015.

[16] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey", *IEEE Communications Surveys & Tutorials*, Vol. 18, pp. 1287-1309, 2016.

[17] A. O. Alkhamisi and S. M. Buhari, "Trusted secure adhoc on-demand multipath distance vector routing in MANET", In: *Proc. of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications*, pp. 212-219, 2016.

[18] I. Kaur and A. Rao, "A Framework to improve the Network Security with Less Mobility in MANET", *International Journal of Computer Applications*, Vol. 167, pp. 21-24, 2017.
[19] K. Arya and S. S. Rajput, "Securing AODV Routing Protocol in MANET using NMAC with HBKS technique", In: *Proc. of the 2014 International Conference on Signal Processing and Integrated Networks*, pp. 281-285, 2014.
[20] P. Kamboj and N. Goyal, "Survey of Various Keys Management Techniques in MANET", *International Journal of Emerging Research in Management & Technology*, Vol. 4, pp. 166-168, 2015.
[21] K. Sudha, J.P. Ranjith, and S. Ganapathy, "Secure Transmission Over Remote Group: A New Key Management Prototype", *International Journal of Computer Science and Network Security*, Vol. 15, p. 101, 2015.
[22] Y. Park and Y. Park, "Secure Private Key Revocation Scheme in Anonymous Cluster-Based MANETs", *Journal of Korea Multimedia Society*, Vol. 18, pp. 499-505, 2015.
[23] N. Renugadevi and C. Mala, "Ternary tree based group key agreement for cognitive radio MANETs", *International Journal of Computer Network and Information Security*, Vol. 6, p. 24, 2014.
[24] K. Kalambe and S. Apte, "An Exhaustive Survey on Security Solutions in MANETS," *International Journal of Computer Sciences and Engineering*, Vol. 5, pp. 124-131, 2017.
[25] J. Verma, P.K. Shukla, and R. Pandey, "Survey of various Trust based QoS aware Routing Protocol in MANET", *Traffic*, Vol. 137, pp. 34-43, 2016.
[26] R. Dhivya and V. Kavitha, "Secured Client Cache Sustain for Maintaining Consistency in MANET's", *International Journal of Research in Engineering and Technology*, Vol. 3, pp. 483-488, 2014.
[27] P.M. Mafra, J. Fraga, and A.O. Santin, "Algorithms for a distributed IDS in MANETs", *Journal of Computer and System Sciences*, Vol. 80, pp. 554-570, 2014.
[28] T. Bhatia and A. Verma, "Security issues in MANET: a survey on attacks and defense mechanisms", *International Journal*, Vol. 3, pp. 1382-1394, 2013.
[29] B.R.S. Devi, A. George, and A.K. Thomas, "Performance Investigation Of Low Power Radio Duty Cycling Mac For Resource Constrained WSN", *International Journal of Engineering & Technology*, Vol. 7, pp. 93-98, 2017.
[30] S. V. Yerur, P. Natarajan, and T. R. Rangaswamy, "Proactive Hybrid Intrusion Prevention System for Mobile Adhoc Networks", *International Journal of Intelligent Engineering and Systems*, Vol. 10, No.6, pp. 273-283, 2017.