International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S, August 2019

Novel Secured Keys Generation (NSEKG) with User Property based Artificial Bee Colony (UPABC) for IDPS in MANET

B. Ananthi, S. Sutha

Abstract--- Wireless networks are been used now-a-days. The most important fact about wireless network is it is mobile. It is thus used in many fields. One of the most important applications of wireless networks is Mobile Ad hoc NETwork (MANET) in which all the nodes work as both transmitter and receiver. MANETs are used in various fields like military, industry and emergency recovery. In order to provide adequate security against multiple attacks, the researchers are of the opinion that detection-based schemes should be incorporated in addition to traditionally used prevention techniques. Intrusion Detection and Prevention System (IDPS) is an effective defense mechanism that detects and prevents the security attacks at various levels. In recent work a polynomial key is employed for achieving useful key generation process and a polynomial is generated to compute the pair-wise key but it can be easily detected by the attacker so to improve the security in IDPS system, this work proposes the secure routing using Novel SEcured Keys Generation (NSEKG) against IDPS system. This proposal implements with two major keys: Secure Key (SeK) and Sharing key (ShK) creation is performed via the use of the User Property based Artificial Bee Colony (UPABC) algorithm and the frequency based behavior with certainty measurement on routing paths. These SeK and ShK keys creation with UPABC scheme exploits the encrypted value of the packets and the decryption determine whether the route reply is the result of a malicious node or not. The proposed NSEKG -IDPS system is very effective for communication attacks and needs to be gradually improved in order to detect multiple attacks. The performance is evaluated primarily in accordance with the subsequent metrics like Packet delivery ratio (PDR), Routing Overhead (RO), End-End-Delay (E2E), and Throughput.

Keywords--- Multiple Attacks, Self-key, Mutual-key, MANETs, IDPS System, Artificial Bee Colony (ABC).

1. INTRODUCTION

Mobile Adhoc Networks (MANETs) is one of the communication standards for wireless communication. Wired networks needs infrastructure to perform any communications where else MANET does not require any infrastructure to do any communication. Along with the widespread use of cheaper, smaller and more powerful wireless nodes over the past few years, MANETs have received much attention, making it one of the most promising areas of wireless network development. MANETs can be used for various applications like Military, Emergency and rescue operations [1].

In MANET the nodes within the radio range can immediately communicate with each other. The nodes that are not within each other's radio range can communicate with the help of intermediate nodes where the packets are relayed from source to destination. Each node should be configured with a unique identity to ensure the packets correctly routed with the help of a routing protocol of a MANET. And also Quality of Service (QoS) routing is a necessary to improve the performance of MANETs.

In addition to finding the routes from a source to a destination, QoS routing also needs to ensure end-to-end quality, usually in terms of bandwidth or delay [2]. A major challenge for MANETs is the design of a secure and efficient routing protocol that can also ensure the overall quality of service during the routing process as MANET. Most of the previous works have been only concentrated on the quality but not in security .But Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and assume that all nodes are trustworthy and well-behaved. However, in a hostile environment, a malicious node can launch routing attacks to disrupt routing operations or denial-of-service (DoS) attacks to deny services to legitimate nodes.

So to avoid those issues, it is necessary to perform intrusion prevention. Several prevention techniques such as binary responses were introduced to avoid that attack but those prevention techniques cannot be enough now days, the most network systems are unsafe to insider attacks [3]. Subsequently, there are constantly new intrusions emerged that cannot be prevented and intrusion detection and prevention (IDPS) system is an effective defense mechanism that detects and prevents the security attacks at various levels in recent work proposed a polynomial key based system but it will be easily leak to the attackers . So to improve the security here implemented the Novel SEcured Key Generation (NSEKG) prevention is performed via the use of the User Property based Artificial Bee Colony (UPABC) algorithm and the frequency based behavior certainty measurement on routing paths. The self-key with ABC scheme exploits the encrypted value of the sequence number as a normal pattern and the decryption determine whether the route reply is the result of a malicious node or not [4].

Manuscript published on 30 August 2019.
***** Correspondence Author (s)
Dr. B. Ananthi, Associate Professor& Head in Computer Science (UG & PG), Vellalar College for Women Erode, Tamilnadu, India. (e-mail: ananthibalamohan@gmail.com)
S. Sutha, Research Scholar, Vellalar College for Women Erode, Tamilnadu, India. (e-mail: Sutha.s84@gmail.com).

2. LITERATURE REVIEW

Singh, et al [5] proposed an Intelligent Intrusion Detection and Prevention System (IIDPS) is proposed for preventing the ad hoc network from these three types of attacks under the AODV protocol. The proposed mechanism works on the basis of trust management. IIDPS includes a trust manager which categorizes the trust of the network into different categories. Different types of malicious nodes are identified by the behavior classifier based on a predefined threshold and risk factor conditions. The proposed IIDPS is responsible for preventing MANETs from the black hole, flooding, and selective packet drop attacker nodes. At the same time, the proposed prevention system improves the performance of the network in the terms of numerous parameters like throughput, overhead, delay, packet delivery ratio etc. Joshi, et al [6] proposed a system which can detect as well as prevent the malicious attacks. The system is named as Enhanced Adaptive ACKnowledgment (EAACK). EAACK gives a better malicious-behavior-detection than the traditional approaches. EAACK is designed to overcome three of the six weaknesses of Watchdog approach, as, false misbehavior, limited transmission power, and receiver collision. Radha and Rao,[7] proposed an IDPS framework for MANET using image processing techniques under blackhole attack is to solve the issues under blackhole attack, there is a loss of energy which is high at the node resulting in loss of battery backup and also excess of bandwidth may be consumed by the attacker. The attacker is an insider. Among various mobility models to generate mobility patterns the Random waypoint mobility model is used to detect the blackhole attack RREP by providing security services like authentication and confidentiality.

Aranganathan and Suriyakala[8] proposed an agent-based model to address the aspect of intrusion detection in cluster based Mobile ad hoc network environment. The model comprises of mobile agents, which are used to detect intrusions, respond to intrusions, mainly preventing the routing attacks while securing them and distributing selected and aggregated intrusion information to all other nodes in the network in an intelligent manner to compensate the attack. The model is simulated to test its operation effectiveness by considering various performance parameters such as, packet delivery ratio, communication overhead, throughput.

Cardenas et al [9]proposed an algorithm to ensure honest backoffs when at least one, either the receiver or the sender is honest. Then discuss detection algorithms to deal with the problem of colluding selfish nodes. Although have focused on the MAC layer of 802.11, approach is general and can serve as a guideline for the design of any probabilistic distributed MAC protocol. Nadeem and Howarth [10] focused on preventing denial-of-service (DoS) attacks. As an example, consider intruders that can cause DoS by exploiting the route discovery procedure of reactive routing protocols. Show the unsuitability of tools such as control chart, used in Statistical Process Control (SPC), to detect DoS and propose an anomaly-based intrusion detection system that uses a combination of chi-square test & control chart to first detect intrusion and then identify an intruder. When the intruder is isolated from the network we show reduced overhead and increased throughput. Simulation results show that this algorithm performs well at an affordable processing overhead over the range of scenarios tested.

Su[11] several Intrusion Detection System (IDS) nodes are deployed in MANETs in order to detect and prevent selective black hole attacks. The IDS nodes must be set in sniff mode in order to perform the so-called Anti-Blackhole Mechanism (ABM) function, which is mainly used to estimate a suspicious value of a node according to the abnormal difference between the routing messages transmitted from the node. When a suspicious value exceeds a threshold, an IDS nearby will broadcast a block message, informing all nodes on the network, asking them to cooperatively isolate the malicious node. This study employs ns2 to validate the effect of the proposed IDS deployment, as IDS nodes can rapidly block a malicious node, without false positives, if a proper threshold is set.

3. PROPOSED METHODOLOGY

In this section describes the proposed technique of IDPS in MANET based on Novel SEcured keys generation (NSEKG) for each packet of data for secure routing using Secure Key (SeK) and Sharing key (ShK) algorithm based on user property based Artificial Bee Colony (UPABC) optimization algorithm and the frequency based behavior with certainty measurement on routing paths for an effective Intrusion Detection And Prevention System (IDPS) in MANETs. At first here generating two kinds of keys namely Secure Key (SeK) and Sharing key (ShK) is used in this work. Overall architecture of the proposed model is shown in figure 1.

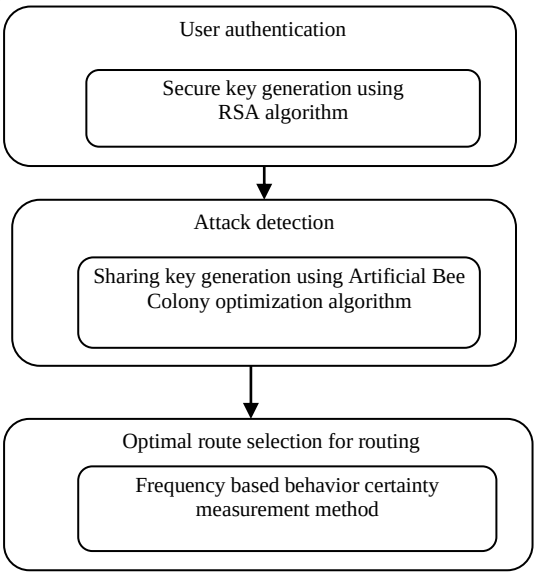

Figure 1: Flow diagram of the proposed system

3.1. Secure Key (SeK) by RSA Encryption

In order to perform the secure key generation first needs to define a system model. Let us consider that the MANET is represented as the Graph G = (V, E), where V is represented as the set of nodes (N) with the purpose of distributed in the network and E is represented as the set of direct edges.

Each E, i.e., a ∀ pair of $N \in V$ may be bi-directional communications. If the node A ϵ V is in the transmission range (TRB) of node B ∈V and vice versa. The direct connection (A, B) ∈ E denotes that the node B is positioned within TR of node A. Node B is an active neighboring node of A, $B \in AN_B$.

The source node N_s initiates the route discovery process to the destination N_d, by broadcasting the RREQ packets with Sequence Number (SN) and Hop Count (HC). The active intrusions involve in communication data dropping, modification, or fabrication to disrupt the normal functionality of routing protocol in MANET. Here the every node in the MANET generates a unique Secure Key (SeK) individually. The data can be encrypted by using the secure key to ensuring privacy. Secure key mechanism to identify the variation of Sequence Number (SN) during the route reply phase. To avoid the additional storage requirement for all nodes SN, instead of encrypting the entire packet, only the dropping intrusion target field is encrypted. The target file of most of the dropping intrusions is a sequence number. During the route discovery process, every receiver applies the Secure Key (SeK). By using the common and pre-stored key value, the receiver behind the Route REPly packet originator can easily verify the misbehavior of a corresponding sender without storing the SN value for every Route REPly process. The packet sender applies the Secure Key (SeK) and attaches the encrypted field in a packet in addition to original SN. The intermediate receiver again encrypts it's with encrypted SN and drops the previous encrypted field of the packet. Every packet receiver repeats this process. The node which is a route to the destination, generating the route reply packet with last received the encrypted packet. The previous hop to the RREP originator verifies the SN value to identify whether it is a dropping intrusion or not. If it is not the intruder, others just forward the reply packet to the sender node without decrypting the packet header [12].

MANET generates a unique Secure Key (SeK) by Rivest–Shamir–Adleman (RSA) algorithm. In this work RSA algorithm is used for encryption, in this a user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, and if the public key is large enough, only someone with knowledge of the prime numbers can decode the message feasibly.

The keys for the RSA algorithm are generated the following way [13]:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random, and should be similar in magnitude but differ in length by a few digits to make factoring harder. Prime integers can be efficiently found using a primarily test.
2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\lambda(n) = \text{lcm}(\lambda(p), \lambda(q)) = \text{lcm}(p-1, q-1)$, where λ is Carmichael's totient function. This value is kept private.
4. Choose an integer e such that $1 < e < \lambda(n)$ and $\gcd(e, \lambda(n)) = 1$; i.e., e and $\lambda(n)$ are coprime.
5. Determine d as $d \equiv e^{-1} \pmod{\lambda(n)}$;i.e., d is the modular multiplicative inverse of e modulo $\lambda(n)$.
   - This means: solve for d the equation $d \cdot e \equiv 1 \pmod{\lambda(n)}$.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $e = 2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.
   - e is released as the public key exponent.
   - d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the private (or decryption) exponent d, which must be kept secret. p, q, and λ(n) must also be kept secret because they can be used to calculate d.

Encryption

To do it, he first turns M into an integer m then computes the ciphertext c, using Alice's public key e, corresponding to.

$$c \equiv m^e (mod\ n) \quad (1)$$

Decryption

The private key exponent d by computing

$$c^d \equiv (m^e)^d \equiv m\ (mod\ n) \quad (2)$$

Given m, she can recover the original message M by reversing the padding scheme

Initially, the node $_{Ns}$ selects the *SN* value and encrypts the self-key. Every RREQ receiver applies this cryptography using its own SeK.

3.2. Sharing Key (ShK) Creation

In this work, Sharing Key (ShK) is generating by using user's very unique properties are Mobile number, Nick name and mail id. **ShK [14]** values are optimized based on the Artificial Bee Colony (UPABC) optimization algorithm by considering the unique properties of user and random number. Random number is generated between the source and destination by random generator for secure communication. Artificial Bee Colony (ABC) is a proposed to solve key optimization process[15]. It was proposed based on forage for honeybees. The process starts when bees leave the hive of forage to search for a food source (nectar). After finding nectar, the bees store it in their stomach. After coming back to the hive, the bees unload the nectar and perform a waggle dance to share their information about the food source and recruit new bees for exploring most rich food sources [16].

```
1: Initialization Phase
2: repeat
3:     Employed Bee Phase
4:     Onlooker Bee Phase
5:     Scout Bee Phase
6:     Memorize the best solution achieved so far
7: until (Cycle = Maximum Cycle Number or a Maximum CPU time)
```

Figure 2: Key Selection

The main steps of the proposed key selection method are illustrated in Figure 2. Each step is described as follows:

1. Create initial food sources: for key selection, it is desirable to search for the best accuracy using the lowest possible number of keys. For this reason, the proposed method follows the forward search strategy. The algorithm is initialized with N food sources, where N is the total number of keys. Each food source is initialized with a bit vector of size N, where only one key will be presented in the key subset, that is, only one position of the vector will be filled with 1.

2. Submit a key subset of food sources to the classifier and use accuracy as fitness: the key subset of each food source is submitted to the classifier, and accuracy is stored as the fitness of food source.

3. Determine neighbors of chosen food sources by employed bees using Modification Rate (MR) parameter: each employed bee visits a food source and explores its neighborhood. For key selection, a neighbor is created from the bit vector of the original food source. In the basic version of ABC algorithm, the neighborhood is defined by performing a small perturbation in only an optimization parameter through Equation 2, which makes convergence slower. In the key selection, the optimization parameters are represented by the bit vectors and their perturbation is performed by a perturbation frequency or MR . For each position of the bit vector or key , a random and uniform number R_i is generated in the range between 0 and 1. If this value is lower than the perturbation parameter MR, the key is inserted into the subset, that is, the vector value at that position is filled with 1. Otherwise, the value of the b it vector is not modified. This is expressed in Equation 3 :

$$X_I = \begin{cases} 1 \text{ if } R_i < MR \\ x_i \text{ otherwise} \end{cases} \quad (3)$$

where x_i is the position i in the bit vector. After selected the optimal key this will be used as a mutual key and it will be shared only to the both sender and receiver so if the attacker hack the self key encryption method to hack the data this mutual key method will be very useful in intrusion detection.

3.3. Frequency Based Behavior with Certainty Measurement

After receiving the Route reply packet either from the destination or the intermediate router, the route discover enables the test forwarding scenario to measure the behavior certainty level of a path. In the model, the N_s send the encrypted dummy data packets to the destination. When the destination node N_d receives a data packet, it adds the ID of successfully received packets in a list L[17]. After t time; the destination sends the list L to the Ns via another route because it is possible that the malicious nodes located in a test path may drop the acknowledgment packet. On the arrival of the packet, the source node Ns extracts the number of received packets ={p_1, p_2,… p_n}, where p_i refers to the identity of a packet. If the value of |p| is closer to the number of sending packets, the selected path is called a normal path. Considering X = {X_1, X_2 ,.. X_n} and X_n is the number of suspected paths that are announced by the neighboring nodes. The path length of X_i is PL_i. The number of node pairs (N_{ij}) appears in the suspected path share PL_{i-1}. Where A is an input node pair, N_{ij} and the Eq. (4) return the result of the number of frequency of node pair in suspected paths. In this way, the route discovers performs intrusion prevention by analyzing the malicious link in suspected paths. According to the behavior certainty value of $path_i$, the source decides the data forwarding path.

$$\text{behaviour uncertainty (A)} = \epsilon(N_{ij} \wedge A) \quad \text{Behaviour certainty } (path_i) = \begin{cases} 0 \text{ if any } A \in PL_i > threshold \\ 1 \text{ else} \end{cases} \quad (4)$$

If it is not trustworthy, the source selects the second shortest path for a test case, and notably, the second path excludes the identified uncertain links. Moreover, this scheme ensures the trustworthiness of a path for data forwarding. However, there remains another issue of data integrity intrusions. Both the implementation of self-key reliant cryptography and appearance frequency based intrusion detection is not efficient to cope up with the data modification and integrity intrusions.

4. RESULTS AND DISCUSSION

EKSC is implemented with NS2 simulator with radio propagation rate 2mbps. In the simulation, use the distributed coordination function of IEEE 802.11 for wireless local area networks as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In the simulation, 100 mobile nodes move in a 1000 × 1000 m region for 100 seconds simulation time. All the nodes have e same transmission range of 250 m. In the simulation, the node speed is fixed as 5 m/s. The simulated traffic is constant bit rate (CBR). The simulation settings and parameters are summarized in Table 1.

Table 1: Simulation Parameter

Parameters	Value
Source Type	MAC
No. of nodes	100
Area size	1000 × 1000
Mac	802.11
Routing protocol	AODV
Radio range	250 m
Simulation time	100 seconds
Traffic source	CBR
Packet size	512 bytes
Packet Rate	5 packets/sec
Mobility model	Random way point
Speed	5 m/s
No. of receivers	5, 10, 15, 20 and 25
Pause time	5 ms
No. of attackers	5
Initial energy	3.3 J
Receiving power	0.395
Transmission rate	250 kb
Simulator	NS 2.34

Performance Metrics

1) *Packet delivery ratio (PDR)*: Points the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

2)**Packet loss ratio(PLR):** Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is measured as a percentage of packets lost with respect to packets sent.

3) *Routing overhead (RO)*: RO defines the ratio of the amount of routing-related transmissions.

4) End-end-Delay: The time taken for a packet to be transmitted across a network from source to destination.

5) Throughput: This is the percentage of sent data packets actually received by the intended destinations.

The simulation results of the various methods with different metrics are discussed in table 2.And by using those metrics and methods white –hat, black-hole; gray whole attacks are detected in this section.

Table 2: Simulation Result of methods in different Scenarios

Packet Delivery Ratio Vs simulation Time					
Simulation Time(seconds)	**TWO ACK**	**EAACK(DSA)**	**EAACK(RSA)**	**EKSC**	**NSEKG**
20	0.8847	0.9026	0.9369	0.9795	0.9895
40	0.8973	0.9103	0.9430	0.9891	0.9991
60	0.9065	0.9256	0.9497	0.9726	0.9926
80	0.9186	0.9370	0.9548	0.9739	0.9939
100	0.9255	0.9417	0.9635	0.9861	0.9961
Packet Loss Ratio Vs simulation Time					
Simulation Time(seconds)	**TWO ACK**	**EAACK(DSA)**	**EAACK(RSA)**	**EKSC**	**NSEKG**
20	5.23	5.01	4.954	3.920	3.102
40	6.071	5.93	5.480	4.933	4.209
60	7.027	6.80	6.540	5.811	5.123
80	8.619	8.20	7.510	7.067	6.457
100	10.8544	9.90	8.700	8.296	7.906
End-to-End Delay (ms) Vs Simulation Time					
Simulation Time(seconds)	**TWO ACK**	**EAACK(DSA)**	**EAACK(RSA)**	**EKSC**	**NSEKG**
20	0.018	0.015	0.014	0.011	0.007
40	0.021	0.016	0.015	0.0123	0.009
60	0.022	0.0168	0.0156	0.0135	0.012
80	0.024	0.017	0.016	0.014	0.013
100	0.026	0.020	0.018	0.015	0.014
Overhead Vs simulation time					
Simulation Time(seconds)	**TWO ACK**	**EAACK(DSA)**	**EAACK(RSA)**	**EKSC**	**NSEKG**
20	1.96	1.58	1.54	1.26	1.01
40	2.93	2.42	2.01	1.40	1.21
60	3.91	3.77	3.06	2.30	1.81
80	4.90	4.59	4.49	3.01	2.72
100	6.09	5.22	5.08	4.25	3.60
Through Put (kbps) Vs Simulation Time					
Simulation Time (seconds)	**TWO ACK**	**EAACK(DSA)**	**EAACK(RSA)**	**EKSC**	**NSEKG**
20	428	440	459	486	495
40	410	420	438	448	467
60	365	379	388	396	421
80	351	360	369	380	401
100	340	352	365	378	395

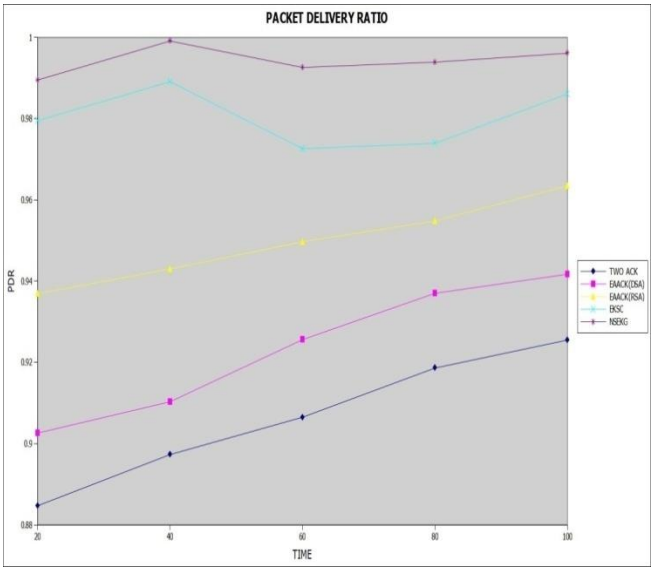

Figure 3: Simulation result of Packet Delivery Ratio Vs simulation time (seconds)

Figure 3 shows the performance comparison results of the packet delivery ratio with respect to five different schemes such as TWO ACK, EAACK (DSA), EAACK (RSA), EKSC[18] and NSEKG. From the results it concludes that the proposed NSEKG scheme produces higher packet delivery ratio results of 0.9961, whereas existing methods such as TWO ACK, EAACK(DSA), EAACK(RSA) and EKSC produces only 0.9255,0.9417,0.9635 and 0.9861 values respectively.

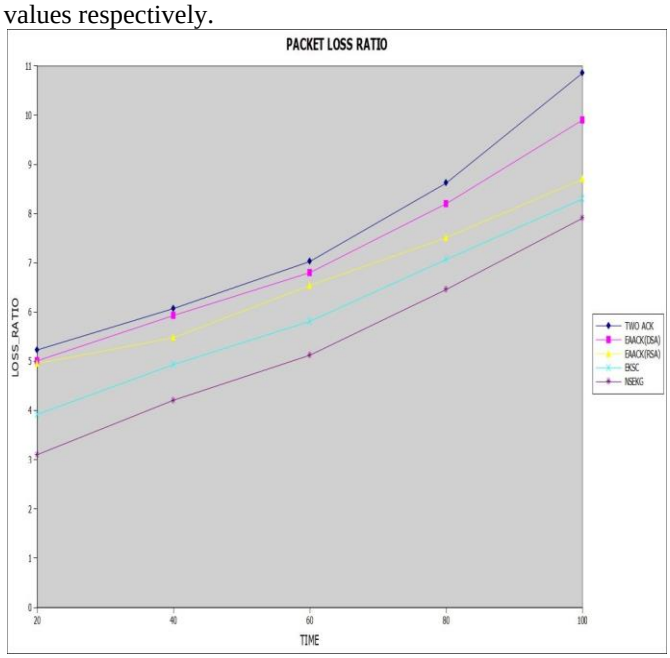

Figure4: Simulation result of Packet Loss Ratio Vs simulation time (seconds)

Figure 4 shows the performance comparison results of the packet loss ratio with respect to five different schemes such as TWO ACK, EAACK (DSA), EAACK (RSA), EKSC and NSEKG. From the results it concludes that the proposed NSEKG scheme produces lower packet loss ratio results of 7.90 whereas existing methods such as TWO ACK, EAACK (DSA), EAACK (RSA) and EKSC produces only 10.85,9.90,8.70, and 8.296 values respectively

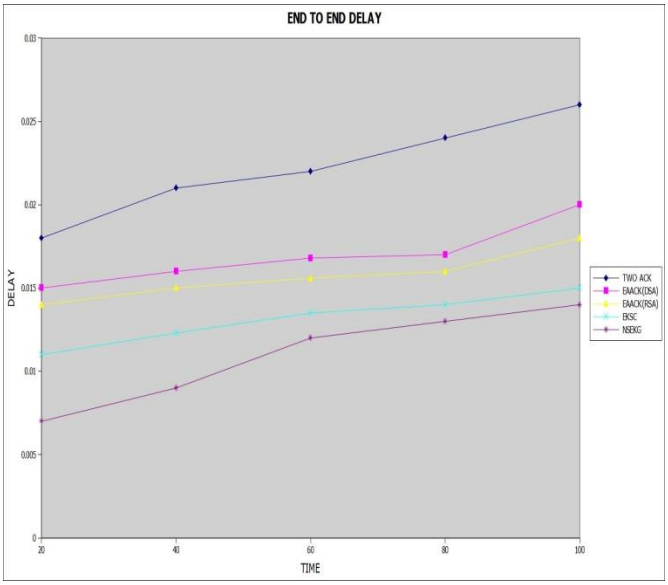

Figure 5: Simulation result of End to End delay Vs Simulation time(10^{-3})

Figure 5 shows the performance comparison results of the End to End delay with respect to five different schemes such as TWO ACK, EAACK (DSA), EAACK (RSA), EKSC and NSEKG. From the results it concludes that the proposed NSEKG scheme produces lesser End to End delay results of 0.14 ms, whereas existing methods such as TWO ACK, EAACK (DSA), EAACK (RSA) and EKSC produces 0.026 ms, 0.020 ms, 0.018 ms and 0.015 ms values respectively.

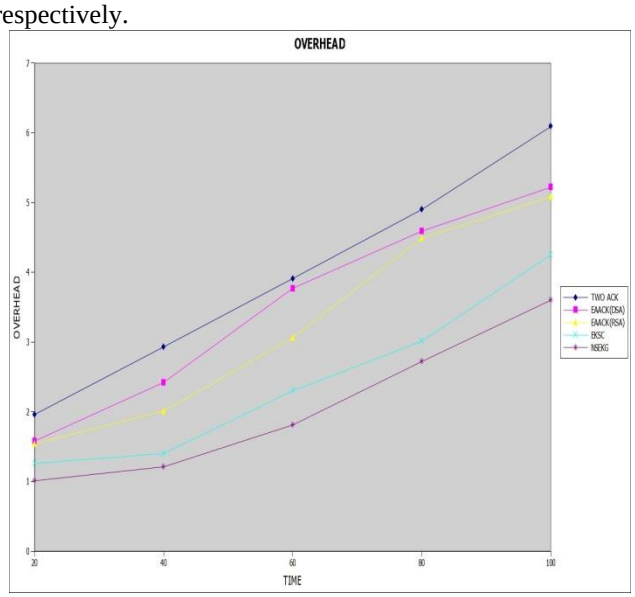

Figure 6: Simulation result of Overhead Vs Simulation time

Figure 6 shows the performance comparison results of the routing overhead with respect to five different schemes such as TWO ACK, EAACK (DSA), EAACK (RSA), EKSC and NSEKG. From the results it concludes that the proposed NSEKG scheme produces lesser routing overhead results of 3.60, whereas existing methods such as TWO ACK, EAACK (DSA),EAACK (RSA) and EKSC produces 6.09, 5.22 ,5.08 and 4.25 values respectively.

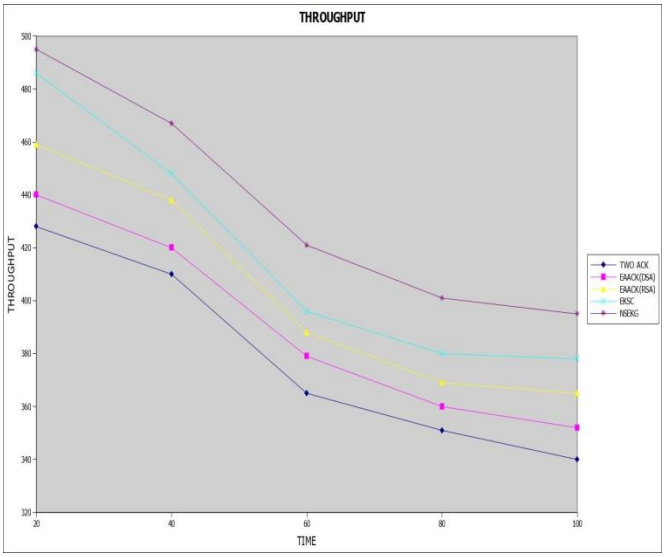

Figure 7: Simulation result of Throughput Vs Simulation Time

Figure 7 shows the performance comparison results of the Throughput with respect to five different schemes such as TWO ACK, EAACK (DSA), EAACK (RSA), EKSC and NSEKG. From the results it concludes that the proposed NSEKG scheme produces higher Throughput results of 395kbps, whereas existing methods such as TWO ACK, EAACK (DSA), EAACK (RSA) and EKSC produces 340 kbps, 352kbps, 365kbps and 378kbps values respectively.

5. CONCLUSION AND FUTURE WORK

One of the most important applications of wireless networks is MANET in which all the nodes work as both transmitter and receiver .In this work two major keys, Secure Key (SeK) and Sharing key (ShK) creation, Novel SEcured Key Generation (NSEKG) is performed via the use of the User Property based Artificial Bee Colony (UPABC) algorithm and the frequency based behavior with certainty measurement on routing paths to detect the intrusion and prevention in MANET. These SeK and ShK keys creation with UPABC scheme exploits the encrypted value of the packets and the decryption determine whether the route reply is the result of a malicious node or not. Performance comparison of the proposed work shows that this work produces the better packet delivery ratio. In future to allow the execution of NSEKG scheme in real time environment to obtain accurate results for testing.

REFERENCES

1. Anantvalee, T. and Wu, J., 2007. A survey on intrusion detection in mobile ad hoc networks. In Wireless Network Security (pp. 159-180).
2. Bao, F., Chen, R., Chang, M. and Cho, J.H., 2012. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE transactions on network and service management, 9(2), pp.169-183.
3. Scarfone, K. and Mell, P., 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST special publication, 800(2007), p.94.
4. Shaojian, S., Jinchuan, W., Xiaofeng, L. and Huixia, L., 2012, Modeling of key production indices and operating parameters optimized set for sugar clarification process. Chinese In Control Conference (CCC), pp. 7113-7118.
5. Singh, O., Singh, J. and Singh, R., 2017. An intelligent intrusion detection and prevention system for safeguard mobile adhoc networks against malicious nodes. Indian Journal of Science and Technology, 10(14),pp.1-12.
6. Joshi, P., Nande, P., Pawar, A., Shinde, P. and Umbare, R., 2015,. EAACK-a secure intrusion detection and prevention system for MANETs. International Conference on Pervasive Computing (ICPC), pp. 1-6.
7. Radha, M. and Rao, C.G., Perusal of intrusion detection and prevention system on a MANET with black hole attack: issues and challenges, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 7, No 2, pp.1-8, 2018.
8. Aranganathan , A. and C.D. Suriyakala, 2018. Agent based secure intrusion detection and prevention for rushing attacks in clustering MANETs. International Journal of Engineering & Technology, 7 (2.20),pp 22-25.
9. Cardenas, A.A., Radosavac, S. and Baras, J.S., 2004, October. Detection and prevention of MAC layer misbehavior in ad hoc networks. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks , pp. 17-22.
10. Nadeem, A. and Howarth, M., 2009, Adaptive intrusion detection & prevention of denial of service attacks in MANETs. In Proceedings of the 2009 international conference on wireless communications and mobile computing: Connecting the world wirelessly , pp. 926-930.
11. Su, M.Y., 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Computer Communications, 34(1), pp.107-117.
12. Burbank, J.L., Chimento, P.F., Haberman, B.K. and Kasch, W.T., 2006. Key challenges of military tactical networking and the elusive promise of MANET technology. IEEE Communications Magazine, 44(11), pp. 39 - 45.
13. Somani, U., Lakhani, K. and Mundra, M., 2010, Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. 1st International Conference on Parallel Distributed and Grid Computing (PDGC), pp. 211-216.
14. Zhao, S., Application of Identity-Based Cryptography in Mobile Ad Hoc Networks. ACM Transactions on Computational Logic, 2007, pp.1-40.
15. 15.Karaboga D, Akay B: A survey: algorithms simulating bee swarm intelligence. Art. Int. Rev 2009, 31(1–4), pp.61-85.
16. Karaboga, D., Gorkemli, B., Ozturk, C. and Karaboga, N., 2014. A comprehensive survey: artificial bee colony (ABC) algorithm and applications. Artificial Intelligence Review, 42(1), pp.21-57.
17. Xia, H., Jia, Z., Li, X., Ju, L. and Sha, E.H.M., 2013. Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Networks, 11(7), pp.2096-2114.
18. Ananthi. B., S. Sutha. 2018. A Novel Encrypted Key based Secure Communication Protocol for Intrusion Detection and Prevention System in Manets. Journal of Adv Research in Dynamical & Control Systems, Vol. 10, 14-Special Issue, pp. 1763-1774.

AUTHOR PROFILE

Dr.B. Ananthi. received her Ph.D. Computer Science in 2011 from Mother Terasa University, India. She has more **than 2**5 years of Teaching Experience and Adding up to her research interest; she has presented and published around 35 Research articles in the National and International Journals. Currently she is a Associate Professor and Head of Department of Computer Science (UG&PG), Vellalar College for Women, Erode. Her current area of research interests are in Image Processing, Adhoc Networks and cloud computing.

S. Sutha received the Bachelor of Science degree in Computer Science from Madurai Kamaraj University in 2004 and her Master degree in Computer Science & Information Technology from the Mother Terasa University in 2007. She completed her M.Phil., degree in the year 2010 from Prist University. She is pursuing Ph.D., in Computer Science at Bharathiyar University. She is presently working in the area of Mobile Security. Other areas of interest include Computer Networks, Mobile Computing, Operating System, Java Programming, Design and Analysis of Algorithms, Software Engineering.