iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3418

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

A Secure Mutually Authentication Scheme in Integration of Internet and MANET based on Chaos Maps

Zara Imtiaz Ali[1], C. Atheeq[2], Arshad Ahmed Khan Mohammed[3]
[1, 2, 3]Department of CSE, [1 ,2]Osmania University, [3]KL University

Abstract**: Integrated Internet MANET (IIM) is a heterogeneous network which is shaped by the interconnection of the wired internet and the wireless mobile ad hoc network. It allows uninhibitedly moving nodes in MANETs to interact with the fixed nodes in internet through the gateway. IIM experiences many security issues due to open wireless medium and lack of mutual authentication between nodes. The existing method provides the security management by data integrity and confidentiality. However, Major disadvantage of symmetric key cryptography is key distribution in network. In MANETs due to mobility and constraint resources key distribution is very much challenging task. Mutual authenticated key agreement technique securely agree on session key between communicating entities, & is also used for secure communication and protection of data from malicious activities. In order to provide mutual authentication between mobile node and a fixed node in IIM, two problems must be overcome i.e. key management and computational cost. Strength of any security algorithm relies on its key management technique with minimum overhead as IIM is resource constraint network. We propose a method to provide mutual authentication between communicating entities using chaos theory. It overcomes the key management cost by avoiding modular exponentiation and scalar multiplications. Moreover our proposed method mutually authenticated key agreement protocol provides a mechanism to securely agree the session key between source and destination. Through extensive simulation analysis, we conclude that the proposed method provides a better approach towards security and protection of data from malicious nodes with minimum overhead in IIM.

Keywords**: Authentication, Chebyshev polynomials, Chaotic Maps, Overhead, Gateway, Security.

I. INTRODUCTION

Desire to connect various portable devices such as laptops, PDAs, smart phones etc with internet at anytime, anywhere and any how lead to the development of wireless networks. Reference [1] Mobile ad hoc networks (MANETs) consist of portable devices such as laptops, mobile phones or personal digital assistants for initiation of communication [2]. A large number of ongoing research and development in the area of MANET is obliged to the single networks and stand alone. Mobile ad hoc networks require the interconnection with internet because a broad range of services and applications depend on wired infrastructure networks now-a-days. Therefore, there is a necessity that ad hoc networks should have access to wired networks along with their services. This interconnection of MANET and internet enhance the plasticity of networking and improve the infrastructure network's coverage area. From the past work like Green Communication, Internet of Things, Machine-To-Machine Networks, Device-to-Device communication, demonstrates a positive approach towards infrastructure less network like MANET to be incorporated into their design was proposed by [3]. The integration connects more elements to both MANETs and Internet proposed by [4]. To connect a mobile node with the external world, it needs to select a gateway. A mobile node can gain access to internet services that are under the coverage of gateway, and the nodes which are not in the range of gateway can access internet by the use of multi hop routing to outreach the gateway through other mobile node as shown in figure 1. The integration attaches additional features for MANETs as well as internet.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

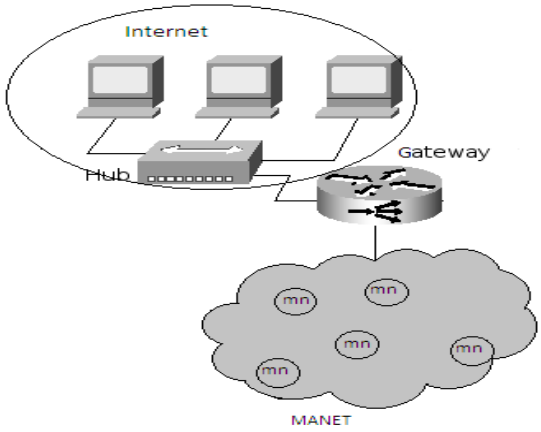


Fig. 1 Internet MANET integration

Security is required in the integrated MANET-Internet environment as it provides more decentralized entry points for malware [5]. Integrating MANETs with internet results in heterogeneous network that create more complexity and new security risks in IIM. An important concept in network security is authentication. Authenticating mobile node with the fixed node in IIM is an important aspect as there are number of decentralized entry ways for malicious nodes to enter into the application domain of MANETs and could misbehave in order to effect the communication between the end parties. So the end nodes which are mutually authenticated can have a secure way to exchange the data that can be protected from misbehaving nodes [6].

Methods by proposed by ([7],[8],[9]) utilized Chebyshev polynomial's for key management to authentication yet they accept that distribution of private data is via some safe medium however it is constrained to MANET. Thus it inspires us to accompany another strategy to give key agreement for mutual authentication in IIM [10]. Our proposed method provides authentication between MN in MANET and FN in internet by sharing a secret session key. We propose a method to provide mutual authentication between communicating entities using chaos theory [11, 12].

The rest of the paper is organized as follows: section 2 describes the related work carried out towards authentication in IIM. Section 3 explains the proposed mechanism for mutual authentication based on chaotic maps. Section 4 shows the results and comparison with existing protocols. Al last we conclude the paper in section 5.

II. RELATED WORK

The most challenging issue in IIM is deploying security as it is integrated and with resource constraint network. For providing security in IIM, the big essential, forthright and pertinent pre requisite is to provide mutual authentication between mobile node and fixed node. The network environment is safeguarded from unauthorized users through the process of authentication and guarantees that the communicating nodes agree on the session key securely. Mutual Authentication in IIM is a security feature in which a mobile node must prove its identity to fixed node and the fixed node must prove its identity to mobile node, before any data traffic is sent. As the network is integrated, the mobile nodes has to first register with the gateway and then authentication between mobile node and fixed node is proved and verified.

ECC, character based, RSA and Diffie-Hellman issue. These protocols assist arranged in light of various characteristics, for example, timestamp, secrecy secret key, Brilliant card and biometric. However these conventions have two key qualifications: ID of vulnerabilities and conquering the vulnerabilities by new strategies. Lately, two gathering confirmed key assertion conventions grew broadly in view of RSA and ECC given by [6]. These conventions endure with overwhelming computational overhead and are not appropriate for IIM compelled asset environment.

Work of [13], proposed a method to provide data integrity in MANETs by symmetric key cryptography incorporating in network layer. Major objective is to provide security to data, when data transfer between communicating entities. This method provides the trust management by data integrity and confidentiality. However, Major disadvantage of symmetric key cryptography is key distribution in network. In MANETs due to mobility and constraint resources key distribution is very much challenging task.

[14]. proposed a mechanism to authenticate the mobile node with the fixed node using chebyshev polynomials. In this paper the composition property is used in generation of the secret key at mobile node as well as fixed node for authentication purpose. The outcome of the mechanism is compared with the existing RSA cryptographic technique in terms of time for generating the secret

key. The proposed model has low computational cost when compared to RSA but the node misbehaviour factors are not considered as mobile node are dynamic in nature and the reason is not justified for dropping the packets.

III. PROPOSED SYSTEM

In our work, the nodes that experience communication are mobile node (MN), gateway (G) and fixed node (FN). Every one of the nodes has 'x' as the public information. If a mobile node needs to communicate with a fixed node, at that point it must be authenticated first with the gateway.

With the aim to provide mutual authentication between a mobile node in MANET and a fixed node in internet, the gateway should first authenticate whether the mobile node is authentic or a malicious user. Later gateway gives mutual authentication between mobile node and the fixed node to upgrade the security in IIM.

Our work intends to accomplish protective communication with security objective authentication as it is the best way to achieve trustworthiness and non-denial information correspondence between MN in MANET and FN in internet [15]. Chebyshev polynomial's composition property introduced by Mason, J.C. furthermore, Handscomb, D.C. (2002) demonstrates the hypothesis of two element key agreement idea which allows the imparting elements for exchanging open keys by means of unprotected channel and make a secret key among them.

A. Defining Chebyshev Chaotic Maps with its properties

Assuming that the integer and a variable are *n* & *x* respectively in intervals [-1,1]. Chebyshev polynomial $T_n(x)$:[-1,1] → [-1,1] is defined as $T_n(x)$ = cos(*n*arccos(*x*)). Chebyshev polynomial map T_n: *R*□*R* f degree *n* is defined using the recurrent relation given by Lee, C.C. et al., (2013) which is given in eq. no. 1:

$$T_n * x = 2xT_{n-1}(x) - T_{n-2}(x), \quad (1)$$

Where *n*>2, $T_0(x)$=1, and $T_1(x)$=*x*

The first few Chebyshev polynomials are:

$$T_2(x) = 2x^2 - 1,$$
$$T_3(x) = 4x^3 - 3x,$$
$$T_4(x) = 8x^4 - 8x^2 + 1,$$
… … … …

Semi group property is an important property of Chebyshev polynomials that is formed by satisfying the eq. no. 2 as

$$T_r(T_s(x)) = T_{rs}(x) \quad (2)$$

An immediate consequence of this property is that Chebyshev polynomials commute underComposition in eq. no 3.

$$T_r(T_s(x)) = T_s(T_r(x)) \quad (3)$$

For improving privacy, Cai, Z. et al., (2015) proposed the semi-group concept that influence Chebyshev polynomials given in interval [-∞,+∞] . Improved Chebyshev chaotic maps are utilized in developed mechanism as in eq. no 4:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x))(mod N) \quad (4)$$

Where n>2, $x \in (-\infty,+\infty)$, and N is a large prime number. Obviously their relation is represented in eq. no. 5,

$$T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x)) \quad (5)$$

Definition 1**:** Semi-group property of Chebyshev polynomials:

$$T_r(T_s(x)) = \cos(r\cos^{-1}(s\cos^{-1}(x))) = \cos(rs\cos^{-1}(x)) = T_{sr}(x) = T_s(T_r(x))$$

Definition 2**:** Consider the parameters x & y, it's difficult to discover the whole numbers, such that $T_s(x) = y$. It is called the Chaos Map Based Discrete Logarithmic Problem (CMBDLP).

Definition 3**:** Consider *x*, $T_r(x)$&$T_s(x)$, it's difficult to find$T_{rs}(x)$=y. It is called the Chaos Map Based Diffie-Hellman Problem (CMBDHP).

B. Hash Function

The properties of Hash Function h: a→b in cryptosystem are as follows:

1) The method *h* accepts the data content of subjective size as input & generates the data content digest of non-variable size as output;
2) The method *h* is uni-directional as provided *a* ,which is simple to calculate $h(a) = b$ nevertheless, provided *b* , which is difficult to calculate $h^{-1}(b) = a$;
3) Consider a and its computing is not feasible to discover *a* ' with the end goal that $a' \neq a$,but $h(a') = h(a)$;
4) Calculations are not feasible to output the pair *a*, *a*' with the end goal that $a' \neq a$, but $h(a') = h(a)$.

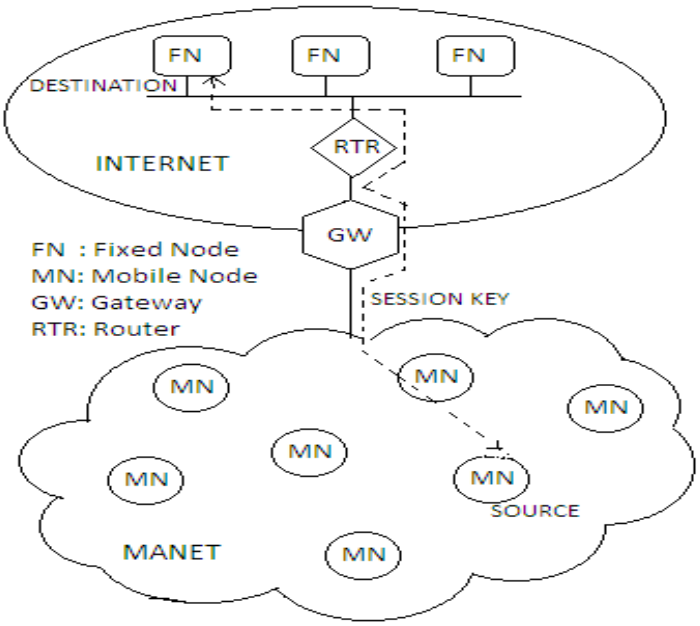


Fig. 2 Session key establishment between mobile node and fixed node

In figure 2, let MN be the source mobile node, GW be the gateway and FN be the destination fixed node.
Expecting that the source MN is reliable and the password is being shared in a secure channel, we are dispensing with the intermediate malicious nodes that effect the integrity of data being exchanged and constraining the internal attacks through the secret key sharing mechanism that is computed by chebyshev polynomials.
It is assumed that the MN, GW and FN share the password in a secure channel.

Mobile Node	Gateway	Fixed Node

Select a secret prime no. 'm'
and compute: $T_m(x)$

$m1 = \{ID_m, ID_f, x, T_m(x)\}$ →

Select a secret prime no. 'g' and compute: $T_g(x)$

← $m2 = \{ID_g, ID_f, x, T_g(x)\}$

Generate
$K_{mg} = (T_m(T_g(x)))$
$H_{mg} = H(ID_m \,||\, ID_g \,||\, ID_f \,||\, T_g(x) \,||\, pw_{mf})$
$C_{mg} = E_{k_{mg}}(H_{mg})$

$m3 = \{C_{mg}\}$ →

Generate

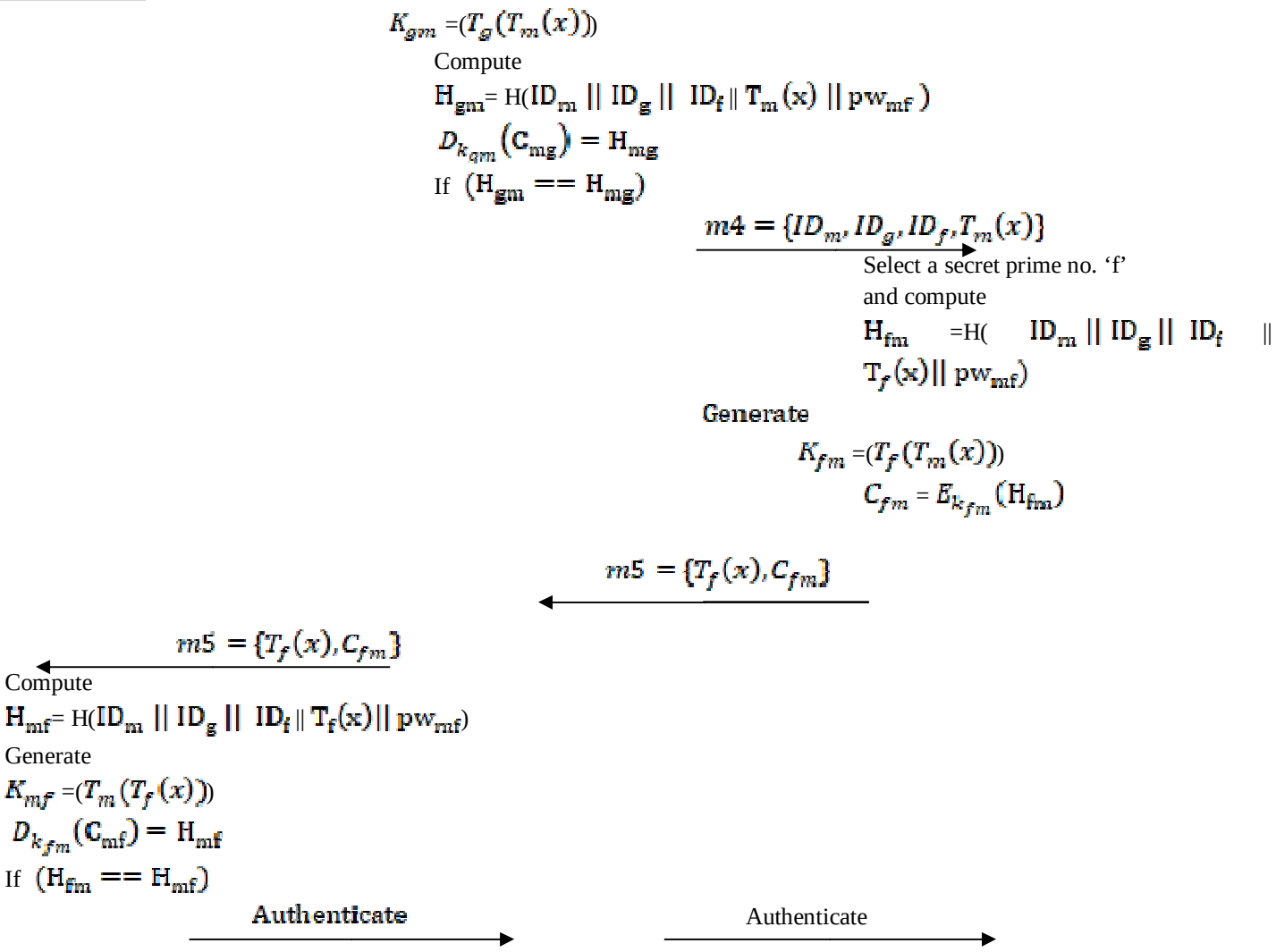


Fig. 3 Mutual Authentication between mobile node and fixed node through Gateway

MN selects a secret Prime number as 'm' and computes $T_m(x)$ and sends it to the GW along with its identity ID_m and public information x in the message m1.

$$m1 = \{ ID_m, x, T_m(x)\}$$

GW selects a secret Prime number as 'g' and computes $T_g(x)$ and sends it to MN along with its identity ID_g and public information x in the message m2.

$$m2 = \{ ID_g, x, T_g(x)\}$$

MN receives the message m2 form GW and generate the key K_{mg} as K_{mg}=($T_m(T_g(x))$) then applies the hash functions for the values ID_m, ID_g, ID_f, $T_g(x)$ and the password pw_{mf} by performing XOR operations on them as H_{mg}= H(ID_m || ID_g || ID_f || $T_g(x)$|| pw_{mf}) Where ID_m, ID_g and ID_f are the identities of MN, GW, and FN that are publicly available. Then MN encrypts the resultant hash value with the key K_{mg} as C_{mg} = $E_{k_{mg}}(H_{mg})$ finally it sends the message into the GW that includes the identities of sender and receiver along with the cipher text as C_{mg}

$$m3 = \{ID_m, ID_f, C_{mg}\}$$

it then compares the resultant H_{fm} with the value it has calculated K_{mf}. If both the values are equal then it authenticates with the FN through GW.

The flow chart for working of proposed mechanism is represented in figure 3.

IV. RESULTS

The proposed model is developed using NS2.34 & examined the overall performance of proposed model by comparing with the existing models. We evaluated the overhead of proposed model with respect to key size variation in mobile nodes of MANETs. For evaluation we have taken into account the scenario in such a manner that mobile node wants to communicate with correspondent node via gateway.

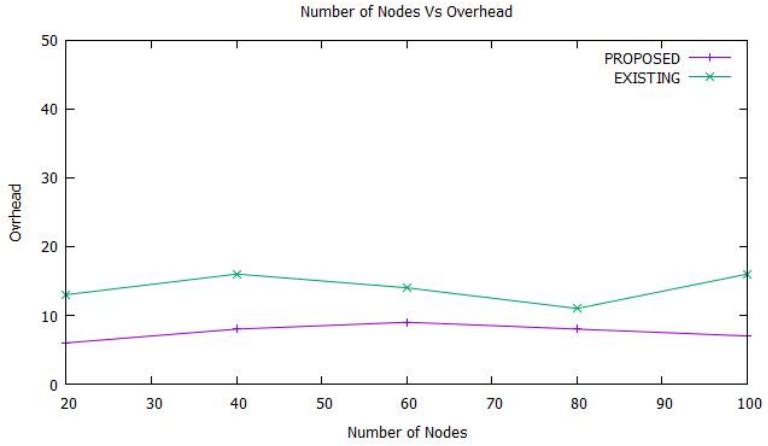


Fig. 4 Comparison of Computational Overhead verses Number of Nodes

In the above graph we have measured the computational overhead of proposed system, as the number of nodes increases the proposed model consumes less overhead when compared to the existing system.

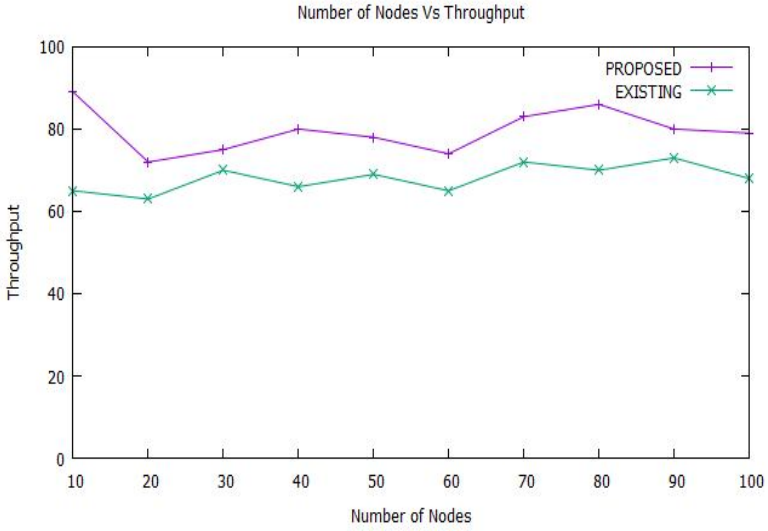


Fig. 5 Comparison of Computational Throughput verses Number of Nodes

In the above graph we are measuring the throughput of the network. The result shows that the throughput of the proposed system is more than the throughput of the existing system. Thus the proposed system gives better results than existing systems.

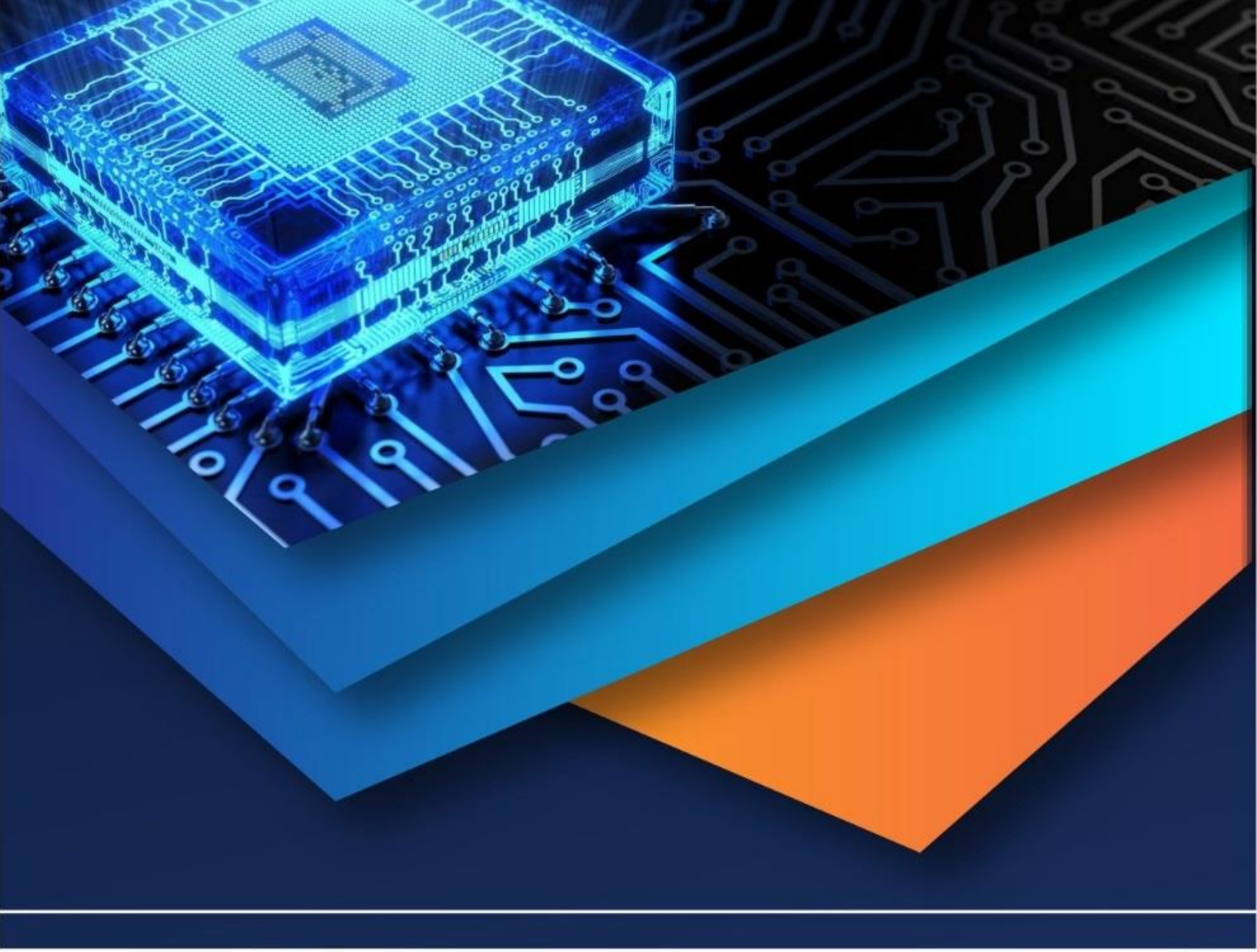
V. CONCLUSIONS

Our work presents a secure mutual authentication scheme in integration of internet and MANET based on chaos maps. We propose a mutual authenticated key agreement protocol for IIM based on chaotic maps by sharing the password in a secure channel. The significant commitment of the work as takes after is key management and computational cost. It overcomes the key management cost by avoiding modular exponentiation and scalar multiplications.The algorithm shows better performances compared to existing

protocols in IIM. The proposed method has very less computational overhead compared to existing method. Also results shows that the proposed method has high throughput than the existing approach.

REFERENCES

[1] Melaku, H.M., Woldegebreal, D.H. and Raimond, K., 2015. Investigating the effects of security attacks on the performance of TCP variants and routing protocols in MANET. International Journal of Computer Applications in Technology, 51(3), pp.235-246.
[2] Siddiqua, A., Sridevi, K. and Mohammed, A.A.K., 2015, January. Preventing black hole attacks in MANETs using secure knowledge algorithm. In Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on (pp. 421-425). IEEE.
[3] Khan, J., Bojkovic, Z.S. and Marwat, M.I.K., 2011. Emerging of mobile ad-hoc networks and new generation technology for best QOS and 5G technology. In Communication and Networking (pp. 198-208). Springer, Berlin, Heidelberg.
[4] Jisha, G., Samuel, P. and Paul, V., 2016. Role of gateways in MANET integration scenarios. Indian Journal of Science and Technology, 9(3).
[5] Atheeq, C. and Rabbani, M.M.A., 2016. Secure Data transmission in integrated internet MANETs based on effective trusted knowledge algorithm. Indian Journal of Science and Technology, 9(47).
[6] Tahat, N., 2016. Convertible multi-authenticated encryption scheme with verification based on elliptic curve discrete logarithm problem. International Journal of Computer Applications in Technology, 54(3), pp.229-235.
[7] Zhu, H., 2015. Flexible and password-authenticated key agreement scheme based on chaotic maps for multiple servers to server architecture. Wireless Personal Communications, 82(3), pp.1697-1718.
[8] Zhen, P., Zhao, G., Min, L. and Li, X., 2014. Key agreement protocol based on extended chaotic maps with anonymous authentication. Chaotic Modelling and Simulation (CMSIM0), 3(3), pp.221-31.
[9] Cai, Z., Feng, Y., Zhang, J., Gan, Y. and Zhang, Q., 2015. A Chebyshev-Map Based One-Way Authentication and Key Agreement Scheme for Multi-Server Environment. International Journal of Security and its Applications, 9(6), pp.147-56.
[10] Mohammad, A.A.K. and Atheeq, C., 2016. Mutual authenticated key agreement scheme for integrated internet MANETs. International Journal of Engineering Applied Sciences and Technology, 1(12), pp.25-28.
[11] Atheeq, C. and Rabbani, M.M.A., 2017. Mutually authenticated key agreement protocol based on chaos theory in integration of internet and MANET. International Journal of Computer Applications in Technology, 56(4), pp.309-318.
[12] Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks. Indian Journal of Science and Technology, 9(26).
[13] Toradmalle, D., Cherarajan, K., Shedage, M., Dogra, N. and Gawde, S., 2016, March. A Secure Protocol for Trust Management in OLSR. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (p. 51). ACM.
[14] Zeba, Kauser and Atheeq C., Performance Based Comparison Study of RSA and Chaotic Maps in MANET. SSRG International Journal of Electrical and Electronics Engineering (SSRG-IJEEE), 2017. Vol. 4, Issue 2.
[15] Atheeq, C. and Rabbani, M., 2017. Secure Intelligence Algorithm for Data Transmission In Integrated Internet MANET. International Journal of Computer Science & Applications, 14(2).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY