

A RESEARCH ON SECURE ROUTING USING CLUSTER BASED KEY MANAGEMENT SYSTEM.

Sweety Patel, Sanket Patel

M.E Student, Kalol Institute of Technology, Gujarat, India.

Asst. Professor, Kalol Institute of Technology, Gujarat, India.

ABSTRACT

Mobile ad hoc network (MANET) is a seamless integration of nodes that can be sender, recipient or relay and may unaware until they come in contact with each other in a decentralized network. Communication should takes place in a secure manner even with the changes on topology, bandwidth, network size, resources etc. The core aspect of establishing trust among the mobile nodes can do with the help of authentication check by exchanging keys. MANETs are vulnerable to attacks and this can be reduced by employing a cluster mechanism which ensures that packet transmission occurs without unnecessary delay. We try to incorporate a new approach in Clustered MANET by implementing a cryptographic technique to tackle the vulnerabilities of the network. This cryptography is highly secure which uses Advanced Encryption Standard(AES) Algorithm with intensify key. This technique can ensure that data is securely transmitted in a reliable manner. This scheme aims at transmission efficiency and also tries to reduce the intruders in Clustered MANET.

Keyword:- mobile ad-hoc network(MANET), s-ack, intensify key, secure digital signature number, Advanced Encryption Standard(AES), Authentication.

1. INTRODUCTION

Wireless network services and applications have always been vulnerable due to the nature of their architectural setup. This unstable nature of wireless networks cannot be stated as an excuse for slack security measures. Vulnerable or not the data transmitted must maintain its integrity and the confidentiality of the sender. Authentication and authorization are the two faces of data security which otherwise can be interpreted as the integrity and confidentiality of data. This dual aspect of security is only possible with the inclusion of strong cryptographic techniques that can safeguard the transmitted data with virtually unbreakable cryptographic codes that helps the network to secure itself against intruders. Cryptography can be symmetric or asymmetric. Symmetric cryptography uses the same keys for encryption and decryption. When the keys used for encryption and decryption are different, it is known as asymmetric cryptography. Asymmetric cryptography provides far more security than symmetric since the sender and the receiver are not aware of each other's private keys.

2. INTENSIFY KEY –DEFINITAION

Intensify keys are generated as the demand arises for sending cryptic text and is formed by stringing together a sequence of complex keys [2]. The name intensify is given to indicate the fact that the key is indeed a one time key that is generated and is never repeated for future uses. IK can be looked at as a onetime pad which is unique for each use. As far as distribution is concerned the unique keys are generated online by the participants in the exchange. A dynamic key generation scheme is used to produce a sequence of dynamic keys from initial parameters. These parameters can either be pre-shared or exchanged via key exchange protocol only once at the beginning of the session. Mathematically, a sequence of Intensify keys is presented as follows:

$$[IKey_i] = \{ IKey_1, IKey_2, IKey_3, IKey_4, IKey_n \} \quad \text{where } 1 < i < n \quad (1)$$

Where: n : number of Intensify keys in a sequence

IKey : intensify keys

[IKey_j] : sequence of intensify keys

The sequence of dynamic keys is required to have minimum risk under cryptanalysis attacks.

3. EXISTING APPROACH (CLUSTRED MANET)

we suggested a cluster based authentication scheme by the formation of clusters under the control of a cluster head. By implementing a cluster based network we were able to prove that data transmission would be efficient and energy of the network would also be saved. The Cluster Head is selected by conducting an election to decide which one of the nodes would be a CH. The CH is responsible for maintaining the information related to a cluster. This information includes the number of nodes currently in the cluster and the routes to each of these nodes. The CH maintains communication with its own members as well as members of other clusters via other cluster heads. Gateways are also used for this purpose. The cluster members communicate to their cluster head.

The communication in a cluster involves three basic steps. The CH

1. receives data from all its members
2. compresses the data
3. transmits the data to the Base station or other CH

Cluster Head selected by the Cluster Head Selection Algorithm.

An efficient CH has the ability to conserve energy and also to improve the network performance. The communication between the members of a cluster and the CH is achieved by sending ACK packets to the CH. These ACK packets can be SACK or 2ACK packets which follows the EAACK approach. The CH receives the ACK., Packets from all members and compress it and sent to the Base Station (BS).

4. PROPOSED SYSTEM

The proposed system aims at secure transmission of data and protection from any intruder who tries to get hold of the data during the transmission. We aim to achieve this by implementing a highly secure cryptographic-AES-algorithm.

Data Confidentiality

Data Integrity

Strong Authentication

Access control of information in CEAAACK.

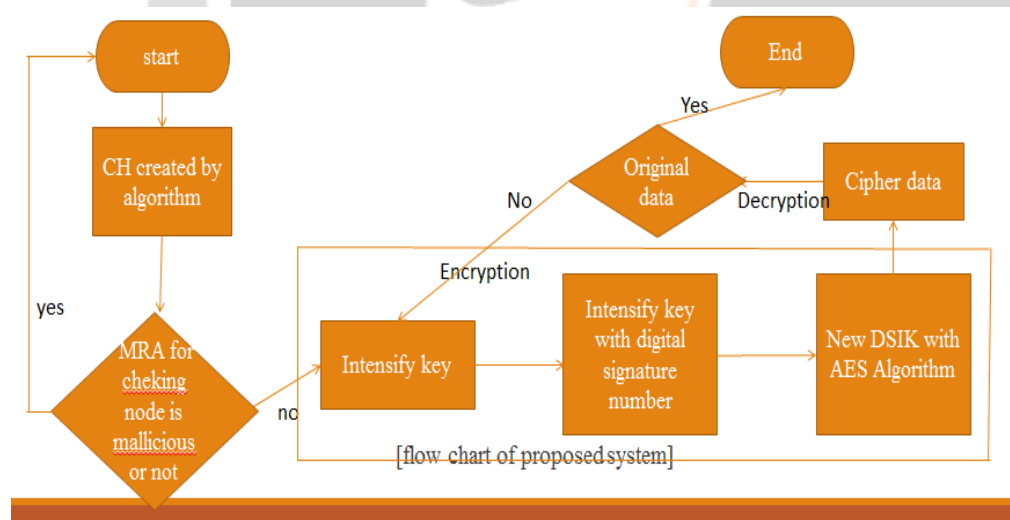


Fig : flow chart of proposed system

Select the nodes from network and create a cluster.

Use a cluster head selction algorithm for selctiong a CH node.

CH get the S-ack from the all nodes, than it compress and sent it to the BS of that cluster.

Now in encryption process intensify key is generated.

Intensify key is merged with the secure digital signature number.

Now this merged key known as the new Intensify key.

This new Intensify key is merged with AES algorithm.

Than encryption and decryption process done.

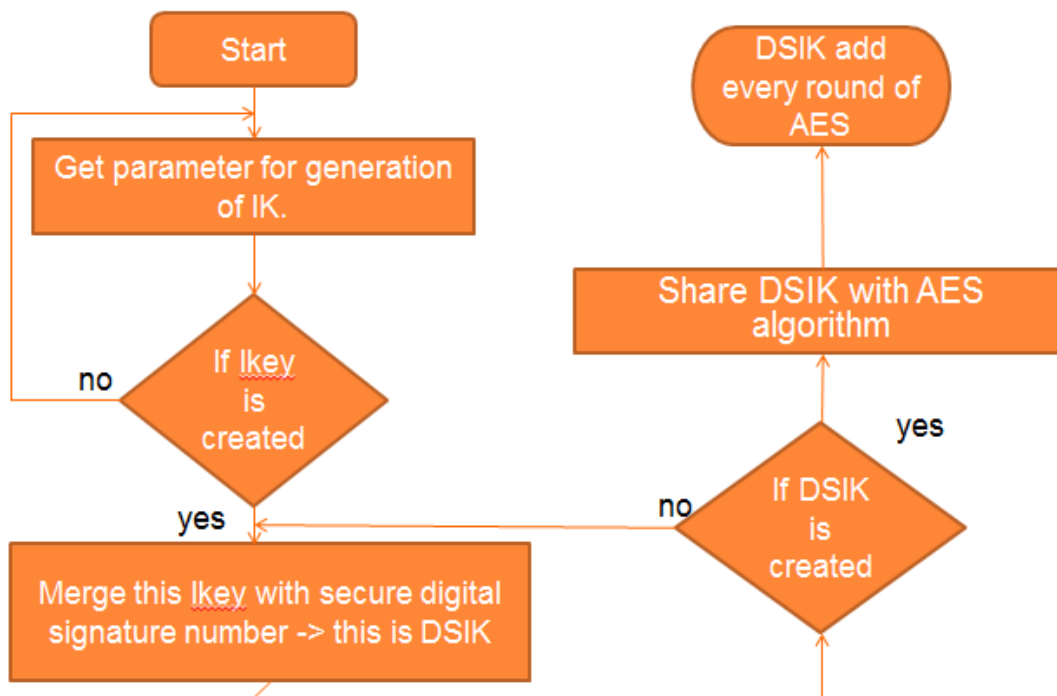


Fig 2: intensify key generation

○ Parameters consider for generating intensify key are.

- Source id
- Port number
- Network time (upto nano second)
- Message id
- Sequence number
- Secured digital signature number
- Message split.

○ Process

○ Sender side:

1. Original data
2. Encryption. ← Using DSIK
3. Cipher text.

○ Receiver side:

1. Cipher text
2. Decryption ← Using DSIK
3. Original data.

5. ANALYSIS OF NETWORK

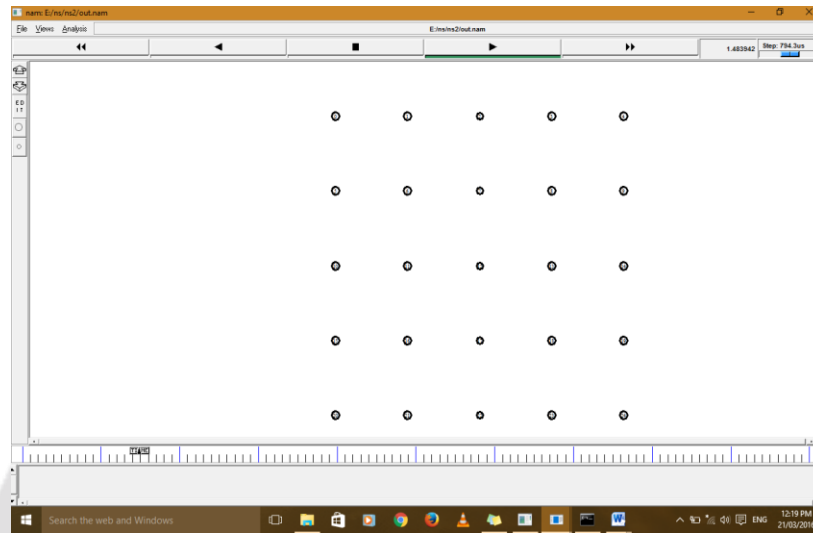


Fig 3: node selection in network

Figure 3 describes that how random node selected in network. Figure 4 shows that channel establishment between sink nodes. Figure 5 shows message passing in 2.0 ms.

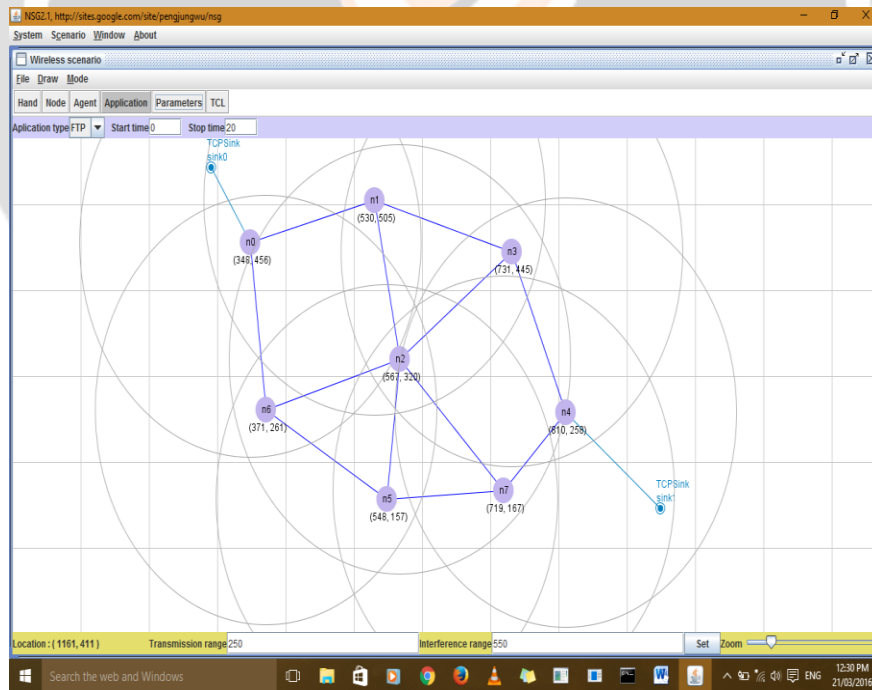


Fig 4: channel establishment

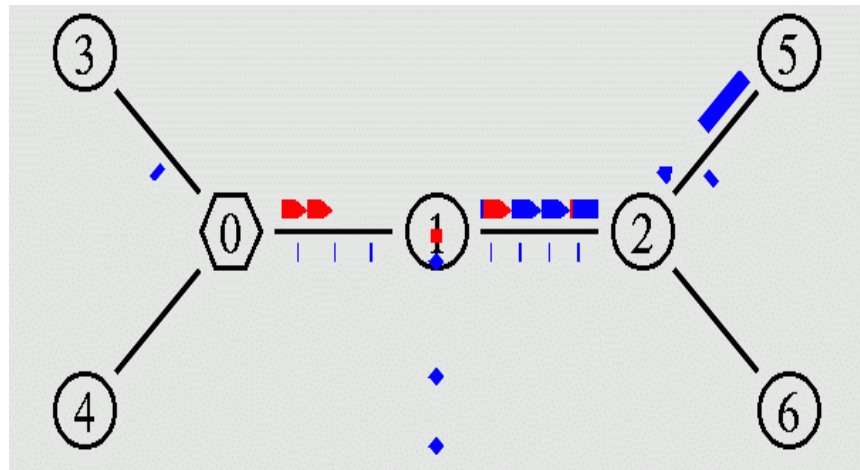


Fig 5: message passing.

6. CONCLUSION AND FUTURE WORK

In this research paper, we have proposed an efficient Intensify key with AES algorithm which is used to filter the attackers in the network and selects only genuine nodes for reliable data transmission. In figure we saw that how algorithm checks the possibility of CH and then select a most probable CH. CH it self not able to check the vulnerability of network, so BS also involve to check the node detection technique.

In future we plan, For instance we plan to conduct a thorough investigation on how to modify this scheme to adapt to other routing schemes and open networks. Research is also planned to extend the intensify key to advance digital signature techniques to avert all possible attacks on the network. Instead of attempting intensify key in a simulated environment, such as NS2, plans are underway to implement the scheme in a real time environment.

7. ACKNOWLEDGEMENT


My sincere thanks to my guide MR. Sanket Patel, who guide me proper in my way of working on this research, without him may I am not able to reach this stage.

8. REFERENCES

- [1] T.Mekala, N.Madhu Suganya” Secure Transaction Using Dynamic Session Key “International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-4, March 2013
- [2] Chinmay K.Nayak (1), G.K.Abani Kumar (2), Parida (3), Das (4),” Detection of Routing misbehavior in MANET with 2ACK schene, Vol.2, No.1, Jan2011
- [3] R.Balakrishna(1), M.Muralimohan Reddy(2), U.Rajeswar Rao(3),G.A, Ramachandra(4), “Detection of Routing Minbehavior in MANET”, using 2ACK”, IEEE International Advance Computing Conference(IACC 2009),Patiala,India,6-7 March 2009
- [4] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE” EAACK—A Secure Intrusion- Detection System for MANETs” IEEE Transactions on Industrial Electronics, VOL. 60, NO. 3, MARCH 2013.
- [5] Sunil V. K. Gaddam, and Manohar Lal “Efficient Cancellable Biometric Key Generation Scheme for Cryptography”, International Journal of Network Security, Vol.11, No.2, PP.6169,Sept.2010.
- [6]D. Djenouri, L. Khelladi, and N.Badache, “A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks,” IEEE Surveys & Tutorials, vol. 7, no. 4, 2005,pp. 2–28.
- [7] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
- [8] I. Chlamtac, M. Conti, and J. J.-N. Liu, “Mobile Ad Hoc Networking: Imperatives and Challenges,” Ad Hoc Networks, vol. 1, no. 1, 2003, pp. 13–64.
- [9] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in Proc. 2001 Advances in Cryptology, pp. 213–229, 2001.
- [10] K.C.ShyamalaBai, “Variable Size Block Encryption using Dynamickey Mechanism (VBEDM)”, IJCA -Volume 27– No.7, August 2011.
- [11] Hamid Mirvaziri, Kasmiran Jumari Mahamod Ismail and Zurina Mohd Hanapi, “Message Based Random Variable Length Key Encryption Algorithm” Journal of Computer Science 5 (8): 573-578, 2009.

[12] Zhu Shun-le, Wang Ya-xiang, Li Xin, “Design and Analysis of Variable-length Block Encryption Based on Chaos Particle Swarm”, Hefei, China. August 24–27, 2010.
[13] H. Chien and R. Lin, “Improved ID-Based Security Framework for Ad Hoc Network,” Ad Hoc Networks, vol. 6, no. 1, 2008, pp. 47–60.

BIOGRAPHIES

	Student of M.E Computer Engineering , Kalol Institute of Technology, Ggujarat, India
	Assistant Professor of Computer Engineering in Kalol Institute Of Technology, Gujarat, India

