ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Improved Key Management in MANETS using Neural Networks

Naresh Kumari
Scholar
Dept. of Computer Sc.& Engg
U.I.E.T., M.D. University, Rohtak, India

Yudhvir Singh
Professor
Dept. of Computer Sc.& Engg
U.I.E.T., M.D. University, Rohtak, India

Barjesh Kochar
Professor
CSE, Bhagwan Parshuram Institute of Technology,
Delhi, India

Abstract: MANETS are highest implemented these days. Due to the ease of implementation, flexibility of deployment, they find their usage in every walk of life. Commercial applications are even larger in number. The transmission of data packets need to be secured on a node to node basis. Neural Networks provide a good and safe identity management for all such communication. In the present work, we provide simulations of data transmission between devices of MANETS, and find how much the neural networks are helpful in packet transmission.

Keywords: MANETS, Neural Networks, Key Management

INTRODUCTION

A MANET is a most encouraging and quickly developing innovation which depends on a self-sorted out and quickly sent system. Versatile Ad Hoc Networks (MANETS) are remote portable hubs that helpfully shape a system without framework. At the end of the day, specially appointed systems administration permits gadgets to make a system on request without earlier configuration [1]. Along these l ines, hubs inside a MANET are included in steering and sending data between neighbors, in light of the fact that there is no coordination or configuration preceding setup of a MANET. MANETs are self-configuring systems of versatile hubs without the nearness of static foundation [2]. They can likewise be enhanced, which implies that all hubs don't have a similar limit in term of assets (power utilizations, stockpiling, calculation, and so forth.). Because of its extraordinary elements, MANET pulls in various true application zones where the systems topology changes rapidly.

It is vital to recognize the properties or qualities of portable specially appointed systems (MANETs). The qualities [3] of MANETs and the conceivable applications are emphatically related; diverse applications request MANETs with variations of the given attributes.

There is nofixed or previous framework in a specially appointed system: all system capacities (steering, security, arrange administration, and so on.) are performed by the hubs themselves. Because of the hubs restricted telecom run, information spread is accomplished in a multi jump mold; hubs can hence be considered as hosts and switches. Hub versatility and remote availability permit hubs to suddenly join and leave the system, which makes the system undefined [4].

CRYPTOGRAPHY AND KEY GENERATION

Encryption is a component by which a message is changed so that lone the sender and beneficiary can see. Typical example of Alice and Bob communication is where Sway gets Alice's message and, utilizing his private-key, decodes it

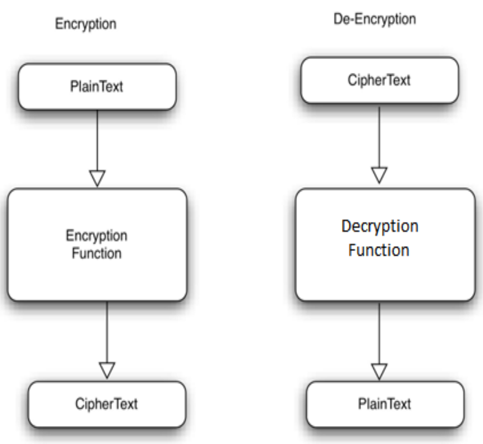

Figure 1: Encryption/Decryption Process Private Key Generation

Symmetric encryption, otherwise called private-key encryption or mystery key encryption, includes having a similar key for encryption and decoding process. The Encryption includes applying a calculation to the information to be scrambled utilizing the private key to make them flighty. The scarcest calculation XOR can make the framework almost sealed.

KEY MANAGEMENT SCHEMES

A keying relationship is the state wherein organize hubs share entering material for use in cryptographic components

[5]. The keying material can incorporate open/private key sets, mystery keys, instatement parameters and non-mystery parameters supporting key administration in different occurrences. Key administration can be characterized as an arrangement of methods[6,7] and strategies supporting the foundation and upkeep of keying connections between approved gatherings.

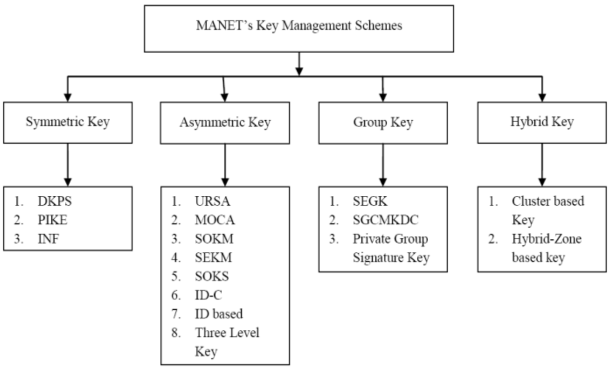

Fig. 2: Key Management Schemes

EXPERIMENTAL SETUP:

For the present work, the neural network setup in Matlab is given below:

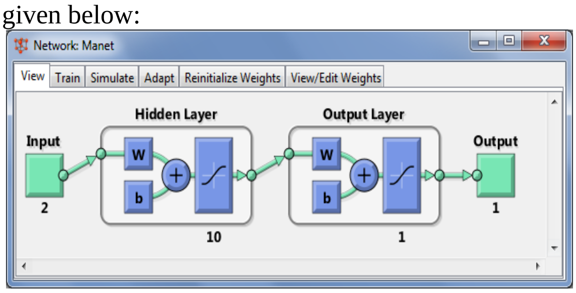

Fig 3: Structure of Back propagating Neural Network with output layers

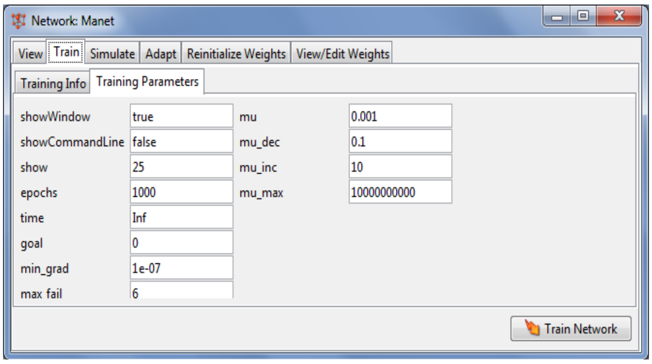

Fig 4: Simulation Parameters for training neural network

RESULTS

Table 1 Values obtained from the trained network at different test points
(μ = 0.001, μ_ dec = 0.01, μ _ inc =10))

Input	Target Value	Trained Value
260	0.34209	0.38656
1107	0.40697	0.45988
144	0.84123	0.95059
691	0.42568	0.48101
793	0.11869	0.13412
500	0.92936	0.93865

Table 2 Values obtained from the trained network at different test points
(μ = 0.001, μ_ dec = 0.001, μ_ inc = 10)

Input	Target Value	Trained Value
911	0.43862	0.49564
318	0.48904	0.55261
187	0.8689	0.98186
1110	0.47186	0.53321
111	0.16434	0.18571
612	0.97089	0.9806

Table 3: No of Nodes vs Required Hidden layer size and Average Delivery Probability

Nodes	HL = 5	HL = 10	HL = 15	HL = 20	HL = 25	HL = 30
40	0.85	0.83	0.8	0.53	0.55	0.71
60	0.87	0.85	0.83	0.55	0.57	0.75
80	0.86	0.86	0.82	0.55	0.56	0.77
100	0.88	0.85	0.84	0.54	0.6	0.79
120	0.87	0.86	0.83	0.57	0.61	0.8
140	0.88	0.88	0.85	0.55	0.62	0.82
160	0.88	0.86	0.86	0.58	0.63	0.81
180	0.88	0.88	0.86	0.59	0.64	0.83
200	0.92	0.92	0.89	0.56	0.64	0.85
220	0.9	0.9	0.9	0.56	0.59	0.86
240	0.95	0.95	0.93	0.57	0.62	0.9

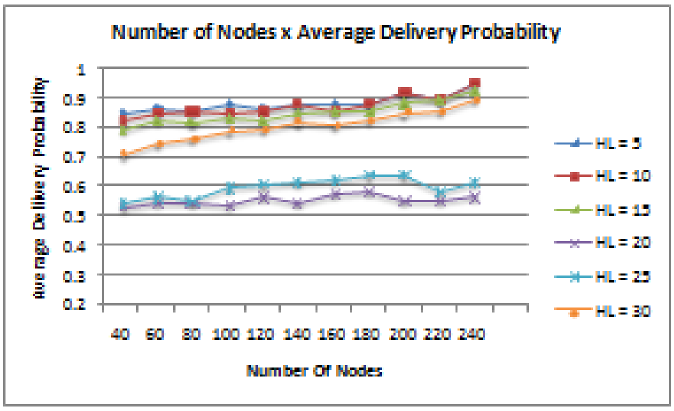

Fig 5: No of Nodes vs Required Hidden layer size and Average Delivery Probability

CONCLUSION

The results of simulations help us conclude that the key management using Neural Networks is a faster and secure system. Table 3 and Figure 5 clearly show that in case of 40 to 240 nodes in a MANET the experiments are successful. The delivery probability is high. This support our hypothesis that if implemented commercially, it is practically viable with high level of integrity and delivery probability.

REFERENCES

1. Kamna Solanki, Yudhvir Singh, "Importance of Selecting Test Cases for Regression Testing", IOSR Journal of Computer Engineering, ISSN: 2278-8727, Vol 16, Iss 4, pp 43-51, Jul – Aug. 2014.
2. Pankaj Lathar, Yudhvir Singh, Girish Kumar Sharma A Novel and Efficient Approach to Retrieve Data from Cloud, International Journal of Computer Science and Engineering, ISSN: 2347- 2693, Vol 2 , Issue 7, pp101-104 July 2014.
3. Pankaj Lathar, Yudhvir Singh, Girish Kumar Sharma Role of Aneka Cloud Application Platform in Growing Market, Journal of Global Research in Computer Science, ISSN 2229-371X, Vol 5, No. 6, pp 33-39, June 2014.
4. Yudhvir Singh, Surbhi Sangwan, "Resource Allocation Using Combinatorial Approach", Proc. of 2nd National Conference on Advances in Computing Communication Networks and Electrical Systems, India, 2014, pp 109-111.
5. Apeksha Malik, Yudhvir Singh, Dheer Dhwaj, "Network Performance in Wireless Sensor Network", Proc. of 2nd National Conference on Advances in Computing Communication Networks and Electrical Systems, India, 2014, pp 310-314.
6. Menal and Sumeet Gill, "An Application of Neural Network for Device Authentication in Bluetooth Pairing Method" in International Journal of Computer Science and Information Technology Research Excellence Vol. 5 Issue 4, Jul. Aug. 2015, ISSN NO. 2250-2734 (Print), 2250-2742 (Online).
7. Menal and Sumeet Gill, Published Research Paper "Enhancing Authentication in Wireless Devices uses Neural Networks" in IOSR Journal, special issue covering National Conference on Recent Trends in Computer Science and Information Technology held at G H Raisoni Institute of Information Technology Nagpur. Indexing Copernicus.