International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-5, March 2019

Protecting Network Routes or Communication by Implementing Secure and Energy-aware Framework in MANETs

Loie Naser Mahmud Nimrawi

Abstract: ***The Mobile Ad hoc Networks (MANETs) very popular at present world and also this MANETs are facing several problems which related security. Security means, network security as well as network data security problems. To avoid such type of problems, we have several protocols for secure routing or secure communication in the MANETs. However, all implemented protocols provide either security to the network data or protect networks from the various attacks. But, no one protocol provides the parallel solution to this existing problem. So, we implemented a framework in existing, named as Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN) which can protect the network and network data from the attackers as parallel. But, SUPERMAN framework can only protect the network routes and its communication data. It cannot balance the network levels of the network nodes in MANETs. Hence, in this paper we are extending that the SUPERMAN framework by adding energy balancing scheme. Through this extension work, we can prove that the proposed mechanism is an energy-aware as well secure framework for MANETs.***

Index Terms**:** ***MANETs, Routing, Network Security, Energy balancing.***

I. INTRODUCTION

MANET is an ordinary multi-hop wireless networks that comprising of computing and communication with numerous cellular nodes. Each node of MANET acts as a sender, receiver as well as a router some times. Majority of routing protocols in MANET performs on the nodes in a network will coordinate to every other at the same time as forwarding information packets to other nodes. But intermediate nodes can also cause numerous issues, can extract beneficial records packets, deny route packets, can additionally adjust the packets contents up to the duration of the records transmission session. The intermediate nodes stated above are of type misbehaving nodes or malicious nodes. This problem will be stopped using cryptography through which authenticating all routing control packets, in order that the out of doors attackers can't involve inside the route discovery system. Security is an essential trouble inside the incorporated MANET-Internet environment because in this environment we ought to keep in mind the attacks on Internet connectivity and additionally on the ad hoc routing protocols. MANET community is tough studies region due to its dynamic topology and power constraints previously for the couple of years. This restricts variety of every cellular nodes security and wireless transmissions troubles and many others. If we tolerate in mind about independent MANET whose connectivity is limited and it has limited packages. Person having MANET have higher use of network sources with respect to the Internet with new protection threats on MANET. Although security has lengthy been a lively research subject matter in wired networks, the precise characteristics of MANETs gift a new set of nontrivial challenges to safety design. These challenges include untie network structure, shared wireless medium, stringent source constraints, and extraordinarily dynamic community topology. The final aim of the security answers for MANETs is to offer security evinces, which includes authentication, confidentiality, integrity, anonymity, and openness, to mobile customers. Network operations may be easily threatened if communications aren't embedded into fundamental network capabilities at the early stages of their layout. Routing community using committed nodes to support simple functions like packet forwarding, routing, and network management, in ad-hoc networks the ones features are completed by way of all available nodes. This could be very tough for the core of the security issues unique to ad-hoc networks. As opposed to dedicated nodes of a classical community, the nodes of an advert hoc network can't be relied on for the best execution of critical network functions. In wireless network there's a high requirement for protection. In this paper we focused on not only security to the MANETs routing security but also providing energy balancing to the network nodes to enhance the network lifetime in future for MANETs.

II. RELATED WORK

The need of security get right of entry to manage in MANET is widely admitted with the aid of one of a kind authorities mainly by way of protection and military agencies for ensuring comfy conversation on network where the nodes aren't equally relied on. S. Maity and S. K. Ghosh offered a framework for imposing coverage based get entry to control safety of MANET. The safety guidelines are upheld by predefined distributed trust parameters set by way of the administrator at the same time mobility of nodes. The predominant powers in their framework are access manage policy modeling; consider incorporation and policy enforcement in MANET.

Manuscript published on 30 March 2019.
***Correspondence Author(s)**
Dr.Loie Naser Mahmud Nimrawi, Department of Computer Systems and Complex Networks, College of Science and Arts, Sajir, Shaqra University; Kingdom of Saudi Arabia.

Their framework also deploys coverage based admission control and cryptographic key trade that allows making sure authentication, confidentiality and depended on communication in MANET. Darren Hurley-Smith et.al proposed an idea to defend the networks but these protocols only defend routes or communique, no longer both. Portable impromptu systems are described by specific topologies because of uncontrolled hub versatility, restricted and variable shared faraway channel transfer pace, and far flung devices forced by means of sequence control. One of the important thing difficulties in such structures is to plan lively directing conventions which are talented, this is, deplete fewer overhead. Another set is on-request directing protocols for transportable impromptu structures has been created with the goal of proscribing the steering overhead. These conventions responsively locate and hold up simply the required publications, rather than proactive conventions which maintain up all courses paying little heed to their use. The key normal for an on-request conference is the supply-commenced course disclosure technique. At something point a movement of a supply needs a direction, it begins a direction disclosure that's processed with the aid of sending a course ask the purpose (more often than not by way of a machine extensive surge) and sits tight for a route answer. Each route revelation surge is associated with crucial idleness and overhead. This is in particular valid for full-size structures. Thusly, for on-request directing to be feasible, it is captivating to keep the path disclosure recurrence low. Sathish kumar et.al tended to the problem of connection reserving and diminishes the no of transmission by using restricting the regular lengthy manner. Because of the confusion of connection scheduler, gift the multiuser keen most severe weight calculation for interface making plans for faraway systems. And moreover consist of the bounce ideal calculation for limiting the regular lengthy manner. In a given device diagram the associated parameter; multiuser community pooling circumstance is decided for without dropping within the transmission method. In mild of this circumstance decided greater parameter i.e., nearby pooling component for choose the manner broke down by means of the avaricious maximum severe weight calculation in remote system diagram.

III. FRAMEWORK

A. Overview Proposed System

In the MANET, security is very crucial thing to protect network data and network connections. The traditional framework i.e., SUPERMAN is our motivation to implement the Energy-aware and secure framework for MANETs.

The designed SUPERMAN framework addresses authentication of node, access control of network, also secure communication using existing routing protocols for MANETs. At the network layer, this framework combines routing with communication security. This framework differs with existing approaches which gives only routing or communication security. In existing methods multiple protocols are required to protect the network.

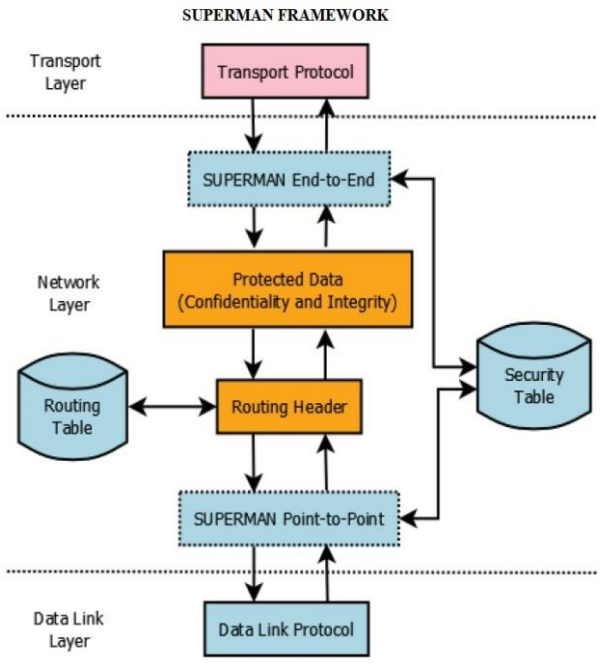

Figure 1: Proposed SUPERMAN Framework

But, we have one more requirement for the MANETs that is we need to enhance the network lifetime for better performance along with secure routing. Hence, in this paper, we are enhancing SUPERMAN framework by implementing energy efficient scheme. While sending a packet from the source to destination without any changes in the routing protocols, the SUPERMAN framework provides a secured communication fully for MANETs. Here, along with security, energy of the nodes is also very significant because without energy to the network nodes, we cannot send or receive the data. So, our proposed framework can efficiently detect the energy levels of the node before sending the data through the path. Which nodes are having more energy in the network with less distance from the source to destination; those nodes will be selected as routing nodes to the packet transmission in the MANETs. By doing this mechanism, we can prolong the network lifetime and we can provide high message delivery ratio with secure routing and secure data communication.

Security

Network Access Control (NAC) recognized as a protection size inside a MANET and is addresses indirectly. To outsider's community, the problem of assumed understandings is avoided.

Shutting the network requires a technique for allowing nodes to agree to accept and leave the shut network. Genuine nodes can be identified by authentication. By the utilization of a certificate to check that they extent a depended on power, nodes may moreover validate one-some other basically dependent on their common Trusted Authority (TA).

Discretion and range mixed and applied in cryptographic set of rules will give rise to an encrypted payload(EP).While at ease records is circulated over more than one hops, it Should be simple.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

This is accomplished the usage of a hashing set of rules consisting of HMAC. Thus the packet's transmission from factor-to-point till the destination is reached is pragmatic.

B. Energy Balancing

Generally, the total energy consumption in two different workloads;

1) The energy consume per packet, which is the ratio of the complete energy utilization over the number of received or delivered data packets
2) The energy consume per hop, which is the ratio of the total energy consumed over the number of hops.

So, while sending packet through the routing path we have to aware about the number of nodes in the network and packet size to know the required energy to transfer packet.

This is possible by our implementation because, we used which nodes having more energy which is estimated from the remaining energy levels of the network nodes.

IV. SOME COMMON MISTAKES

In our experiment, we used a Trusted Authority (TA) server to verify the authority of the network nodes. First, we create a network and we have to discover the routes to transfer the packet from source node to destination node.

Figure 2: Trusted Authority (TA) server to verify the authority of the network nodes

While sending data from source to destination, the data will be sent as HMAC code. If any attacker may attack on our network, the proposed framework can detect the attacker.

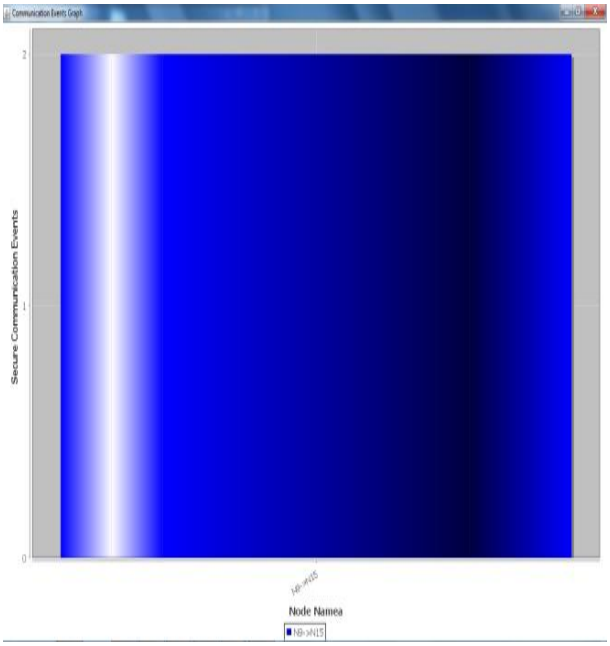

Figure 3: Shows secure communication events from source node to destination node

From the above graph, we see that the secure communication events from source node to destination node. As in case of Convolutional neural networks for better quality of images can be obtained whereas SUPERMAN is used for better quality transmission of packets from one node to another nodes with high security.

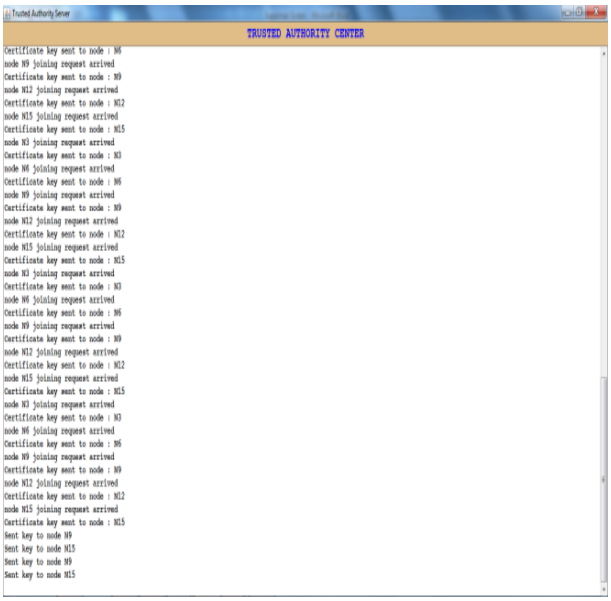

Figure 4: Trusted authority server showing every authentication action

Finally, we can see the every authentication action will be recorded at trusted authority server.

V. CONCLUSION

Finally, our conclusion is, in this paper we motivated from the SUPERMAN framework and we extend this framework with energy efficient scheme.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

By using the only SUPERMAN framework, we can provide or protect the network data and network routes from the attackers. But, through our extension work, we also achieved that the energy-aware and secure routing network in the MANETs. From the experimental results, we proved that the proposed mechanism is secure and energy efficient more than existing frameworks.

REFERENCES

1. S. Maity and Ghosh, "Enforcement of access control policy for mobile ad hoc networks," in Proceedings of the Fifth International Conference on Security of Information and Networks. 2012, pp. 47–52.
2. P. Sathishkumar , S. Balakrishnan , A. Vivek , "HOP Optimal Algorithm With Greedy Link Scheduler, To Avoiding Link Failure For Multihop Wireless Networks", International Journal of Innovative Research & Development Vol 2, Issue 4, April 2013.
3. Park VD, Corson MS. "A highly adaptive distributed routing algorithm for mobile wireless networks" in Proceedings of IEEE 1997.
4. L. Harn, M. Mehta, and W.-J. Hsin, "Integrating diffiehellman key exchange into the digital signature algorithm" Communications Letters, IEEE, vol. 8, no. 3, pp. 198–200, 2004.
5. H. Krawczyk and P. Eronen, "Hmac-based extractand-expand key derivation function" 2010.
6. A. Adekunle and S. Woodhead, "An aead cryptographic framework and tinyaead construct for secure wsn communication," in Wireless Advanced (WiAd), 2012. IEEE, 2012, pp. 1–5
7. R. R. Tewari, and Upadhyay, "Different types of attacks on integrated manet-internet communication," International Journal of Computer Science and Security, vol. 4, no. 3, pp. 265–274, 2010.
8. D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, "A cluster-based approach to consensus based distributed task allocation," in Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euro micro International Conference on. IEEE, 2014, pp. 428–431.
9. R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on. IEEE, 2012, pp. 535–541.
10. Darren Hurley-Smith, Jodie Wetherall, Andrew Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks", IEEE Transactions on Mobile Computing.
11. Gopatoti, A., Naik, M.C., Gopathoti, K.K." Convolutional Neural Network based image denoising for better quality of images", International Journal of Engineering and Technology(UAE), Vol.7, No.3.27, (2018), pp. 356-361.

AUTHORS PROFILE

Dr.Eng. Loie Naser Mahmud Nimrawi is currently working as Assistant Professor in Computer Systems and Complex Networks, College of Science and Arts, Sajir, Shaqra University; Kingdom of Saudi Arabia. He has six years Teaching experience. He received Ph.D in Computer Systems and Networks in the year 2012 from Technical University, Sofia, Bulgaria and Master of Computer Systems Engineering and Technologies in the year 2009 from Technical University, Sofia, Bulgaria. He has received Bachelor of Computer Engineering in the year 2005 from Al-Balqa' Applied University, Amman, Jordan.