Journal of Excellence in Computer Science and Engineering, Vol. 3(2) 2017, pp. 27-33

RESEARCH ARTICLE

Authenticating and Securing Ad-Hoc Networks using Gateway Selection Algorithm

***C Murugamani[1]**

[1]Associate Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad-500 059, Telangana, India.

Received- 7 February 2017, Revised- 12 April 2017, Accepted- 23 May 2017, Published- 16 June 2017

ABSTRACT

Wireless Ad-hoc Networks (WANETs) or Mobile Ad-hoc Networks (MANETs) are vulnerable to different sorts of threats because of their dynamic nature and absence of an essential issue of control. Collaborative attacks happen when numerous attackers synchronise their activities to upset a target network. MANET is an accumulation of nodes in versatility that co-ordinate each other forming a network through wireless connections, in which every node acts a router. The dynamic topology and self-sorting out of the nodes make them more vulnerable against the network. In MANET, the major testing undertaken is to give security amidst directing of information bundles. Different sorts of attacks have been noticed in ad-hoc networks, yet no appropriate arrangement was found for these attacks. In this research, a gateway selection algorithm has been proposed to give node authentication while a new node join the network and before initiating route discovery process in mobile ad-hoc networks. Likewise it is also demonstrated how the proposed method mitigates the effect of attacks on nodes. The result shows a better security level of about 92%. It is found to be higher than other methods.

Keywords: Mobile ad-hoc networks, Gateway selection, Route discovery process, Proactive routing protocols, Reactive or hybrid routing protocols.

1. INTRODUCTION

Networking is an engineering discipline that expects to think about and break down the correspondence procedure among different computing devices or PC frameworks that are connected, or organized, together to exchange data and share resources. Networking relies on the hypothetical application and functional usage of fields like computer engineering, computer sciences, information technology and telecommunication. A computer network is a system in which multiple computers are connected to each other for the purpose of sharing information and resources in some way (e.g. wired (LAN), wireless or internet). Computer networking has existed for about 50 years, with the first computer network developed in the 1960s.

A wireless network is a network that utilizes wireless information associations between different network nodes [1]. Wireless networking is a strategy by which homes, media communication networks and business establishments stay away from the expensive procedure of bringing links into a building, or as an association between different equipment areas. Wireless broadcast communication networks are by large executed and regulated utilizing radio communication. The first wireless network was produced in 1969 at the University of Hawaii and wound up plainly operational in June 1971. The first business wireless network was the WaveLAN. There are different types of wireless networks; they are, Wireless Personal Area Networks (Wireless PAN), Wireless Local Area Network (Wireless LAN), Wireless ad-hoc network or Mobile Ad-Hoc Network (MANET),

*Corresponding author. Tel.: +919941170225
Email address: drcmurugamani@gmail.com (C.Murugamani)
Double blind peer review under responsibility of DJ Publications
https://dx.doi.org/10.18831/djcse.in/2017021003

Wireless Metropolitan Area Networks (Wireless MAN), Wireless Wide Area Networks (Wireless WAN), Cellular network or mobile network, Global Area Network (GAN) and Space networks. Wireless ad-hoc network is the widely used network; in this, research security feature of the ad-hoc network is improved by implementing a gateway selection algorithm.

WANET or MANET is a decentralized kind of wireless network. The network is ad-hoc on the grounds that it doesn't depend on a prior foundation, for example, switches in wired networks or access points in managed (framework) wireless networks [2]. Instead, every node takes an interest in directing by sending information to different nodes so that the assurance of which nodes forward information is made progressively on the premises of network availability and the steering calculation being used. Wireless mobile ad-hoc networks are self-designing, active networks in which nodes are allowed to move [3]. Wireless networks do not have the complexities of framework setup and administration, enabling devices to create and join networks "on the fly" – anyplace, at any time. Figures 1 and 2 show the difference between server based network connection and ad-hock network.

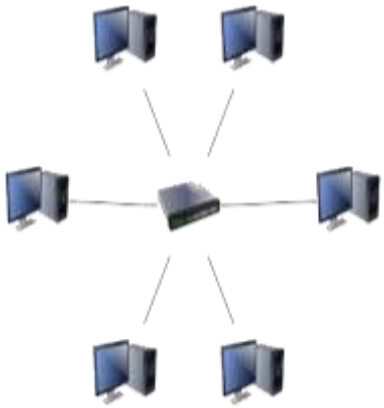

Figure 1.Server based network

The signals of ad-hoc wireless networks are not strong with respect to the utilization of routers that make them function well. Although wireless networks tend to be costlier, they are actually simple to embed [4-6]. Still, securing their signals is the real challenging task because insecure wireless networks are hacked easily. Banks and other such organisations prefer wired to wireless networks, as in these cases, data loss refers to loss of everything. So they are preferred for providing reliable data transfer. But wireless signals are easier to catch than wired signals.

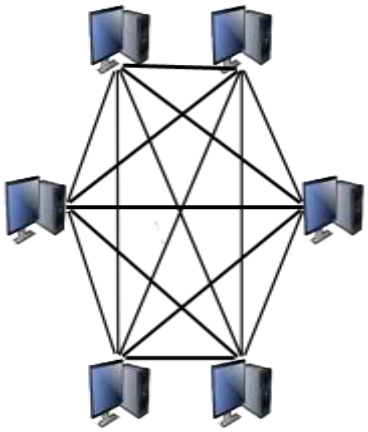

Figure 2.Ad-hoc network

At the point, the wireless ad-hoc signals are hindered by the specific snags such as dividers, gates and hackers when transferring them. The quality of wireless signs relies on the area; in case the user is near to the framework that transmits signals, the transmission rate and quality is high [7]. For instance, a wireless system that is implemented all through an academic structure can't get to all the students because of the signal quality varying from area to area. In other words, entire organisation can't be profited from the single wireless network. An unauthorized client is the greatest worry for individuals exchanging delicate data. The reason is that the client can misuse the network or even hack vital data. The utilization of ad-hoc wireless innovation requires the implementation of additional security. The current upgrade of wireless technology obliges the users to enhance their insight about making use of any wireless innovation in a right way. Although it is popular, it is expensive to stay connected. Further it is less stable and proficient than a wired network, where it works on the rule, the closer the faster. A wireless connection involves a setup of stations, which are the transmission media that assist in the operation of the wireless system [8].

In ad-hoc network lack of security is the main drawback and so we implement gateway selection algorithm for improving the security features. If an attacker comes close to the range of ad-hoc network, he won't have any trouble in connecting to the network. Gateway selection algorithm protects the network

surrounding with a firewall that prevents unauthorised user to access network and also improve the data transfer rate.

Gateway selection can be easily integrated with the routing protocol and provide security [9]. This mechanism is called multi-level authentication technology which includes proactive routing protocols and reactive or hybrid routing protocols. Proactive protocols are the broadcasting gateway i.e. outer layer security of the ad-hoc gateway selection algorithm; The first step is to give permission to enter the network. Reactive or hybrid routing protocols is the ad-hoc's spine network gateway. The features and uses of ad-hoc wireless network are,

- Ad-hoc networks are helpful when you have to share documents or other information specifically with another PC in Wi-Fi range.
- More than one PC can be associated with the ad-hoc network, the length of the greater part of the connector cards are arranged for impromptu mode and interfaced with the same SSID (benefit state identifier). PCs should be within a distance of 100 meters.
- If an individual who sets up the specially appointed system, separate from the system, the various clients are disengaged. A specially appointed system is removed when everybody on it separates, which can be great or awful, contingent upon the view; it's really an unconstrained system.
- One can utilize ad-hoc remote network to impart the network connection with another PC.

2. LITERATURE REVIEW

A vast amount of literature is available, where selective encryption algorithm concepts have been reviewed.

[10] showed a probabilistic selective encryption algorithm which uses the upsides of the probabilistic strategy that intends to obtain extra vulnerability. [11] proposed one selective encryption algorithm to manage the on-going security necessities. One bit selection algorithm to choose the higher extraordinary bits to accomplish higher visual debasement is presented. [12] displayed a near investigation of generally utilized symmetric encryption algorithms AES, DES, 3DES, and Blowfish as far as power utilization is considered.

[13] proposed a new selective encryption algorithm which associates one to a large number of nodes generally of low-security level. [14] proposed two layer determination plans for selective network algorithms. The algorithm diminishes the computational unpredictability by 50% on an average. [15] reported an upgraded ant based defence mechanism for selective forwarding attack in MANET. A SACK plan to transmit the safe affirmation is actualized. A trust model is intended to recognize attackers. [16] proposed a security answer for the routing protocol OLSR. The framework depends on the asymmetric and dynamic system. The principle reason behind the approach is to secure the activity against potential attacks without diminishing system exhibitions. [17] proposed a server-client application made particularly for two associated framework calling. Its principle design was to actualize a selective encryption algorithm.

2.1. Concept of selective encryption

Selective encryption algorithms are in the mainstream today because of the way they decrease the overhead spent on network encryption/decryption, and therefore enhance the proficiency of the network. In this arena, we introduce the rule of selective encryption and after that give the overview of a portion of the selective encryption approach [18, 19]. The reason for selective encryption algorithms is to encrypt just certain bits of the network, yet at the same time, adequate networks are encrypted to give reliable wellbeing in order to secure the transmitted message privacy. It's a bit much that all networks are encrypted through selective encryption; still, the whole information transmission can be seen to be overall secured. Selective encryption is capable to enhance the versatility of information transmission and furthermore decrease the handling time.

On account of selective encryption algorithms, there is contribution of instability in the network encryption, while deciding the questionable example of an encrypted network. In this manner, vulnerability may improve the security of information transmission, since all networks are accepted to have broken even with significance. In this way, instability ends up plainly to be one of the central components while outlining a selective encryption based cryptosystem. Generally, the more the

vulnerability is included, the more is the success of the cryptosystem [20].

Right now, selective encryption algorithms are primarily connected in the energy-aware environments or vast scale networks, for example, Wireless Sensor Networks (WSNs), MANETs, for network encryption and data transmission. In a WSN, every gadget utilizes the battery as its energy supply and hence has repressed computational capacity, so that it is troublesome for a sensor to spend excessive computational cost on information encryption and decryption. Interactive media correspondence regularly requires on-going security and so vast measure of sound and video information should be transmitted safely.

Limitations of existing work:

- For record and printer sharing, all clients should be in the same workgroup, or in the event that one PC is joined to a domain, alternate clients need to have accounts on that PC in order to access shared items.
- Other limitations of ad-hoc wireless networking include, lack of security and a moderate data rate.
- Ad-hoc mode offers minimal security. If an attacker comes close to the range of the ad-hoc network, he won't have any trouble connecting to it.

Advantages of our proposal methodology are as follows:

- Better security
- High speed data transfer

3. PROPOSED METHODOLOGY

Web accessing of ad-hoc network is mostly attained via the gateway, where the core issues are found in gateway, gateway selection and routing node.

Gateway selection algorithm is a multi-level authentication technology which includes gateway disclosure components: proactive routing protocols and reactive or hybrid routing protocols. In the proactive routing protocols, the gateway notices the frequently broadcasting gateways and during the establishment of the reverse route, ad-hoc networks of portable nodes inside the gateway accept the notice, as per the reverse gateway notice, directing data to refresh their routing. Reactive or hybrid routing protocols facilitates the ad-hoc spine network gateway node to start the request and ad-hoc nodes ask for data broadcast to their neighbours and then their neighbours check the gateway list. Upon receiving the node in a current broadcast notice inside the gateway gap where there is an immediate path to the gateway, at that point the node unicast starts a reply asking for the node; else it sends the demand to their neighbours. This method prevents flooding of broadcast notice that sets the gateway notice for the survival time of a specific number of hops.

The gateways have to register the first mobile node that creates a registration request, including the user address and care of address gateway for accessing the mobile internet gateway node in the message. The gateway, then receives a registration request begun by the node. After this, the home gateway receives the request, and creates a node entry and sets up the table entry effective time. Hence mobile node to the home gateway is required to be registered regularly to update this entry. Then the home gateway sends the registration reply to the requesting node. Nodes accepting the demand reaction are set for the survival time of selection gateways and are allowed to exist prior to their dismissal.

Due to the unique topology of the ad-hoc networks, the gateway maintains highest possible access time that could secure data transmission more efficiently. It should be noted that the ad-hoc gateway node accepts the notification packets in radio form.

3.1. Proposed algorithm

Hops: nodes from the gateway to send the current broadcast hops;

Previous hop: Ad-hoc node upstream neighbours;

TTL: Hybrid system used for the survival time in the gateway notices;

Expiration time: the current valid time of broadcast messages in the gateway and in the gateway broadcast interval

This method is based on security factors, and the effective get to time is the no. of hops.

$$T_a = T_e - T_p$$

$$T_A = \sum_{i=1}^{n} P_i T_{ai}$$

Ad-hoc node receives broadcast information gateway,

```
Start
if (node is currently no access to any gateway)
send a message to set the current gateway for
the node;
else
{
if (broadcast messages from the same gateway)
{
if (r < R)
set the gateway to send the information
recently received the upstream node
upstream of the new node, node;
else
{
if (k < 1)
set the gateway to send the information
recently received the upstream node upstream
of the new node, node;
}
}
else
{
if (k < K)
change the gateway prefix, and set the node
that recently received upstream gateway
information as the new node;
}
}
end;
```

4. RESULTS

In order to observe the characteristics of our proposed method, gateway selection MANET, we carried out an experiment within a wireless environment. The experiment setup is done using three laptops with windows OS and two mobile phones with android OS as shown in figure 3. At first the experiment is done without implementing proposed method. Here the network is connected with five devices, where a new device easily entered the network and hacked all data and destroyed the network without any interception. Next, proposed algorithm is implemented with MANET; again the network is connected with five devices. Now a device enters the network, which is redirected to a page as shown in figure 4. New users need to register the network and they were asked to fill some details as shown in figure 5 to precede including email address, username and password. After completing the details, an alert notification is sent to the current users with all the details including IP address to accept or reject the new network as shown in figure 6. If the user rejects the network, gateway will block the IP address of the new network. If the network is accepted by the user, connection will be established and next time they can connect to the network with the username and password.

Figure 3.Experimental set up

Figure 4.Login page

Figure 5.New network registration page

Figure 6.Security warning window

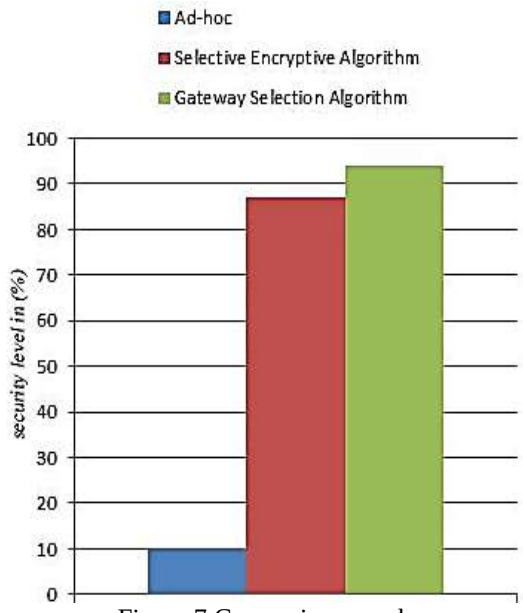

Figure 7.Comparison graph

Table 1.Security level

Networks	Security level in (%)
Wireless ad-hoc network	10
Selective encryption algorithm with WANET	87
Gateway selection algorithm with WANET	92

This research result is compared with existing selective encryption algorithm and the result is shown in figure 7. The security level of selective encryption algorithm and proposed methodology is shown in table 1. This research with selective gateway algorithm gives high security to the wireless ad-hoc network.

5. CONCLUSION

With the consistent research in the field of communication, ad-hoc networks have turned into an innovative research. Ad-hoc network nodes are utilized to grow multi-hop correspondence scope of mobile communication framework and enhance information exchange rates. Keeping ad-hoc network as the access network to the internet, the gateway discovery protocol is vital in choosing the most suitable gateway to ensure the connection between ad-hoc networks and IP-based fixed networks. This research puts forward a gateway selection algorithm which is utilized to secure the connection and to provide stable course to the gateway selection condition. As indicated by the gateway selection algorithm, it develops a quick information exchange method which can diminish the exchange time and enhance the information proficiency, and thus can enhance the nature of communication over the network.

REFERENCES

[1] Y.Xua, J.Liu, Y.Shenc, X.Jiangd and N.Shiratori, Physical Layer Security-Aware Routing and Performance Tradeoffs in Ad-Hoc Networks, Computer Networks, Vol. 123, 2017, pp. 77-87.

[2] S.Khakpour, R.W.Pazzi and K.El-Khatib, Using Clustering for Target Tracking in Vehicular Ad-Hoc Networks, Vehicular Communications, Vol. 9, 2017, pp. 83-96.

[3] M.Rmayti, R.Khatoum, Y.Begriche, L.Khoukhi and D.Gaiti, A Stochastic Approach for Packet Dropping Attacks Detection in Mobile Ad-hoc Networks, Computer Networks, Vol. 121, 2017, pp. 53-64.

[4] J.Feng, X.Du, G.Zhang and W.Shi, Securing Multi-Channel Selection using Distributed Trust in Cognitive Radio Ad-Hoc Networks, Ad-Hoc Networks, Vol. 61, 2017, pp. 85-94.

[5] S.Nikoletseas, T.P.Raptis and C.Raptopoulos, Radiation-Constrained Algorithms for Wireless Energy Transfer in Ad-hoc Networks, Computer Networks, Vol. 124, 2017, pp. 1-10.

[6] V.G.Gopika and Neetha Alex, A Secure Steganographic Method for Efficient Data Sharing in Public Clouds, Journal of Excellence in Computer Science and Engineering, Vol. 1, No. 2, 2015, pp. 11-22, http://dx.doi.org/10.18831/djcse.in/2015021002.

[7] P.I.Basarkod and S.S.Manvi, Mobility and QoS Aware Anycast Routing in Mobile Ad-Hoc Networks, Computers and Electrical Engineering, Vol. 48, 2015, pp. 86-99.

[8] C.Annadura and V.Nagarajan, A Link Selection Strategy for Cooperative Ad-Hoc Networks, Computers and Electrical Engineering, Vol. 48, 2015, pp. 109-118, https://dx.doi.org/10.1016/j.compeleceng.2015.01.006.

[9] S.Liua, P.C.Olveczky and J.Meseguer, Modeling and Analyzing Mobile Ad-Hoc Networks in Real-Time Maude, Journal of Logical and Algebraic Methods in Programming, Vol. 85, No. 1, 2016, pp. 34-66, https://dx.doi.org/10.1016/j.jlamp.2015.05.002.

[10] T.Xiang, J.Hu and J.Sun, Outsourcing Chaotic Selective Image Encryption to the Cloud with Steganography, Digital Signal Processing, Vol. 43, 2015, pp. 28-37, https://dx.doi.org/10.1016/j.dsp.2015.05.006.

[11] W.Wen, Y.Zhang, Z.Fang and J. Chen, Infrared Target-Based Selective Encryption by Chaotic Maps, Optics Communications, Vol. 341, 2015, pp. 131-139, https://dx.doi.org/10.1016/j.optcom.2014.12.026.

[12] T.Xiang, J.Qu and D.Xiao, Joint SPIHT Compression and Selective Encryption, Applied Soft Computing, Vol. 21, 2014, pp. 159-170, https://dx.doi.org/10.1016/j.asoc.2014.03.009.

[13] O.Y.Lui and K.Wong, Chaos based Selective Encryption for H.264/AVC, Journal of Systems and Software, Vol. 86, No. 12, 2013, pp. 3183-3192.

[14] N.Taneja, B.Raman and I.Gupta, Selective Image Encryption in Fractional Wavelet Domain, International Journal of Electronics and Communications, Vol. 65, No. 4, 2011, pp. 338-344, https://dx.doi.org/10.1016/j.aeue.2010.04.011.

[15] E.Damiani, S.C.Vimercati, S.Foresti, S.Jajodia, S.Paraboschi and P.Samarati, Selective Data Encryption in Outsourced Dynamic Environments, Electronic Notes in Theoretical Computer Science, Vol. 168, 2007, pp. 127-142, https://dx.doi.org/10.1016/j.entcs.2006.11.003.

[16] Q.Liang, T.S.Durrani, Y.Pi and X.Wang, Hybrid Wireless Ad-Hoc Networks, Ad-Hoc Networks, Vol. 58, 2017, pp. 1-5, https://dx.doi.org/10.1016/j.adhoc.2017.02.005.

[17] G.Yan and D.B.Rawat, Vehicle-to-Vehicle Connectivity Analysis for Vehicular Ad-Hoc Networks, Ad-Hoc Networks, Vol. 58, 2017, pp. 25-35, https://dx.doi.org/10.1016/j.adhoc.2016.11.017.

[18] S.Umamaheswaran, K.Senthil and R.Rajaram, An Algorithm for Encrypting/Decrypting Textual Messages, Journal of Excellence in Computer Science and Engineering, Vol. 1, No. 1, 2015, pp. 1-10, http://dx.doi.org/10.18831/djcse.in/2015011001.

[19] A.Kushwaha, H.R.Sharma and A.Ambhaikar, A Novel Selective Encryption Method for Securing Text over Mobile Ad-hoc Network, Procedia Computer Science, Vol. 79, 2016, pp. 16 – 23, https://dx.doi.org/10.1016/j.procs.2016.03.004.

[20] M.Hamdi, R.Rhouma and S.Belghith, A selective Compression Encryption of Images Based on SPIHT Coding and Chirikov Standard Map, Signal Processing, Vol. 131, 2017, pp. 514-526.