IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW OF SECURE ROUTING PROTOCOLS FOR IPV6 BASED MOBILE AD-HOC NETWORKS (MANET)

Rakesh Kumar Pal[*1] & Dr. Deepali Gupta[2]
[*1]Maharishi Markandeshwar University, Ambala, India
[2]H.O.D Computer Science Department, Maharishi Markandeshwar University, Ambala, India

DOI: 10.5281/zenodo.1345598

ABSTRACT

The Mobile ad hoc networks (MANET) have become most significant and are being used widely in many applications. Generally, these applications require low cost, low energy and low data nodes that communicating over multiple hop to cover a large geographical area. In internet protocol version (IPv6) based MANETs, the neighbor discovery enables nodes to self-configure and communicate with neighbor nodes through auto configuration so the chances of energy consumption and security of network become high. This paper presents a survey of different routing protocols of IPv6 based MANET to minimize the cost, delay, energy consumption rate. The major dispute in providing connectivity is to minimize the energy consumption of network and provide security in ad hoc routing protocol between nodes and ad hoc networks. There, this paper focuses on comparative analysis of routing protocols with their security and also we briefly describe different ways to provide global security for IPv6 based MANETs.

Keywords: Mobile ad hoc networks (MANET), IPv6, Routing protocols, QoS parameters.

I. INRTODUCTION

Wireless equipment's such as Bluetooth or the 802.11 standards enable mobile devices to set up a Mobile Ad-hoc Network (MANET) by connecting dynamically through the wireless medium without any centralized configuration [1]. MANETs recommend several advantages over traditional networks including reduced infrastructure costs, ease of founding and fault tolerance capability, as routing is performed independently by nodes using other intermediate network nodes to forward packet data from one node to another node [2], this multi-hopping reduces the chance of security. So IPv6 based MANET is introducing by researches which a combination of mobile nodes that dynamically structures a temporary network. It executes without the usage of existing infrastructure with more security by using the concept of Secure Neighbor Discovery (SeND) with Light Weight Cryptographic Address Generation (LW-CGA). Because of the property of self-deliberate, in which every point of network behaves as source or router and moreover every nodes keep moving freely in network area. MANET plays an important role in connectionless system. Security is the primary need in mobile ad hoc network for securing the sensitive information from hackers. In MANET, normally, numbers of attacks are routing protocol attacks. Mobile Ad-hoc system is the kind of system, where communication happens in remote medium utilizing an access point. Different systems like WSN (Wireless Sensor Network) are the systems in which communication happens through physical medium.

MANET is the foremost promising network and multiple access procedure for data transmission because:

- ❖ It is strong to frequency-selective fading,
- ❖ Compensates for the effect of multipath at the receiver node by designing a filters, which can gather the transmitted energy spread over multiple nodes, and
- ❖ Allows receiver nodes to differentiate among signals simultaneously transmitted by multiple transmitting nodes.

For these reasons, MANET increases network reuse and reduces packet retransmissions rate, which results in decreased energy consumption and increased network throughput within the ad hoc network. The Internet protocol version 6 (IPv6)-enabled network architecture has recently attracted much attention. In this paper, we introduce a comparative analysis of MANET routing protocols based on IPv6 with security algorithm that provide better security mechanism during the transmission of packet data.

The Communication in MANET is occurring by utilizing multiple ways [2]. Hubs in the MANET offers the remote medium and the topology of the system changes sporadically also alertly. In movable area, breaking of communication connection is exceptionally less, as hubs are allowed to move to anywhere the thickness of hubs and quantity of hubs are relying on upon the application in which they are utilizing Mobile network. Mobile Ad hoc network have offered ascent to many applications. With numerous applications, there are still some outline issues and difficulties to overcome.

In the below Figure 1, example of typical MANET is given, in which the radio range for every single node is demonstrated by a circle around that specific node. Such that, A can reach D either by following the route A-B-C-D or by A-B-D-C.

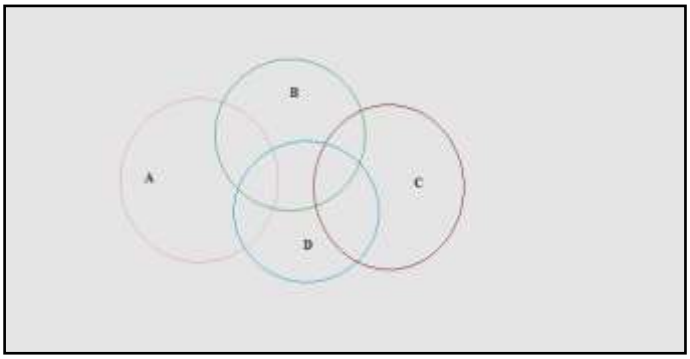

Figure 1: Architecture of MANET

Above figures represent the architecture of MANET to transmit the packet data from one node to other node using routing mechanism. The existing MANET routing technique is allowing a lot of users to distribute simultaneously a finite amount of packet data with less distortion but there is a main concern of security of data. In general, MANETs are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links without using the existing network infrastructure or centralized administration. With the advantage of dynamic topology i.e. the nodes are free to move randomly and organize themselves arbitrarily; such flexibility and convenience do come at price.

Ad hoc wireless networks inherit the traditional problems of wireless communications and wireless networking [10]:

- The wireless medium has neither absolute, nor readily observable boundaries outside of which stations are known to be unable to receive network frames;
- The channel is unprotected from outside signals;
- The wireless medium is significantly less reliable than wired media;
- The channel has time-varying and asymmetric propagation properties;
- Hidden-terminal and exposed-terminal phenomena may occur.

II. CLASSIFICATION OF ROUTING PROTOCOL

Due to the highly dynamic nature of a mobile ad hoc network several frequent and unpredictable changes in network topology are observed which adds difficulty and complexity to routing among the mobile nodes and reduce the security of transmitting packet data. Thus, the significance of routing protocol in establishing communications among mobile nodes, make more secure routing area the most active research area within the MANET domain. Numerous routing protocols and algorithms have been proposed, and their performance under various network environments and security conditions have been studied and compared.

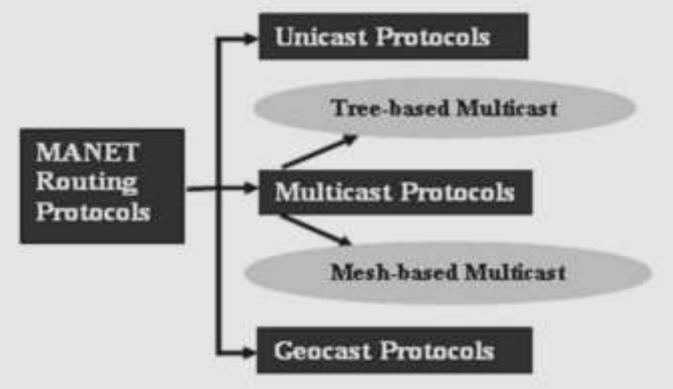

Figure 2: Classification of MANET Routing Protocols

Above figure represent the classification of secured routing protocols in MANET. Unicast routing protocols means a one-to-one communication, i.e., one source node transmits data packets to a single destination node. This is the most prevalent category of routing protocols found in mobile ad hoc networks.

Multicast routing protocols come into use when a source node needs to send the similar message, or stream of data, to multiple destination nodes.

Geo-cast routing protocols are a special case of multicast that is used to distribute data packets to a group of nodes situated inside a specified geographical area of network.

Several surveys and comparative analysis of MANET routing protocols have been published in previous year. A preliminary classification of the routing protocols can be done via the type of cast property, i.e., whether they use a Unicast, Geo-cast, Multicast, or Broadcast forwarding. This segment presents the various aspects of routing algorithms and the following section will provide brief description of various routing protocols and their comparative analysis.

III. ANALYSIS OF DIFFERENT PROPOSALS FOR MANETS

This section explains a glance of existing techniques in the field of IPv6 based MANET for the detection and prevention of attack and help to provide more secure network.

Reshmi, T. R., and K. Murugan [1], proposed "Light weight cryptographic address generation (LW-CGA) using system state entropy gathering for IPv6 based MANETs". The paper proposes empirically strong Light Weight Cryptographic Address Generation (LW-CGA) using entropy gathered from system states. Even the system users cannot monitor these system states; hence LW-CGA provides high security with minimal computational complexity and proves to be more suitable for MANETs. The LW-CGA and SeND are implemented and tested to study the performances. The evaluation shows that LW-CGA with good runtime throughput takes minimal address generation latency. In this work main problem occurs due to the limited bandwidth and processing power. So in this work we need to improve the privacy enable auto-configurable in MANET using more light weight techniques.

JeeHyeon Na et al [2] they proposed self-organization addressing protocol automatically organizes nodes into tree architecture and configures their global IPv6 addresses. Novel unicast and multicast routing protocols, based on longest prefix matching and soft state routing cache, are specially designed for the IPv6-based MANET. Mobile IPv6 is also supported such that a mobile node can move from one MANET to another. Moreover, a peer-to-peer (P2P) information sharing system is also designed over the proposed IPv6-based MANET. They have implemented a prototyping system to demonstrate the feasibility and efficiency of the IPv6-based MANET and the P2P information sharing system. Simulations are also conducted to show the efficiency of the proposed routing protocols.

Ahmed Shariff et al [16] demonstrated that Mobile Ad-Hoc Networks (MANETs) are portrayed by the absence of framework, element topology, and their utilization of the open wireless medium. Black hole attack speaks to a

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

noteworthy risk for such sort of systems. Firstly, it exhibits a broad study of the known black hole discovery and the prevention approaches and another by assessed new measurements for their characterization.

Bikramjeet Singh et al [17] discussed a single and cooperative black hole attack is one of the prominent security enforcement in MANETs where a malicious node spoofs a source node and absorbs a packet for a destination node by facilitating self-designated routes during the route discovery process. Researchers around the world have proposed various detection techniques and schemes to detect this type of security attack. This presented a hybrid technique to mitigate the effects of black hole attacks and maintain a military perspective. The simulation was performed using the NS-2 simulator. The metrics used are delay, throughput, and packet transfer rate.
In this section we describe the simulation results of existing work with their comparisons. The comparison of existing work is given in table on the basis of different routing protocols in the MANET.

Table 1: Comparison of existing work based on Energy Consumption

ROUTING PROTOCOLS	EXISTING WORK
SeND	720 MJ
IP-based core network	842 MJ
DSR	869 MJ
Security based RP	748 MJ

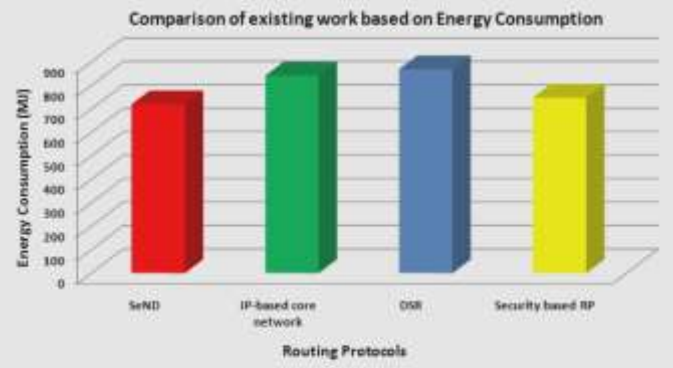

Figure 3: Comparison of existing work based on Energy Consumption

Above table 1 and figure 3 shows the comparison of energy consumption rate using different routing protocols in MANET. From the figure it is clear that the energy consumption rate is better with SeND and Security based routing protocols and it is possibility to combine both techniques for better results.

IV. CONCLUSION

In this work, we introduced a comparative analysis of routing protocols in MANET with security concern. In this survey, we discuss security of IPv6 based MANET and its characteristics, advantages, application, challenges, issues and different types of routing protocols for efficient and effective communication between the mobile nodes participating in a dynamically reputable network of nodes. The discussed routing protocols are roughly classified into three types namely Broadcast, Unicast and Multicast routing Protocols. In this paper, a brief description on secure routing protocols is provided and how they are superior to other existing routing protocols is exposed.

As already mentioned in this survey, the research in the area of mobile ad-hoc networks is future from being comprehensive. Much of the effort is waste on devising routing protocols to maintain the secure and effective transmission of data packets between nodes that are part of the network. However, there are a lot of topics for research in this field like:

- How can ad-hoc network seamlessly and efficiently access the internet in order to provide advanced services for users.
- There is a possibility to improve the Quality of service (QoS) of existing MANET.
- How can the network secure itself from malicious or compromised hosts is a big are for further research.

REFERENCES

[1] Reshmi, T. R., and K. Murugan. "Light weight cryptographic address generation (LW-CGA) using system state entropy gathering for IPv6 based MANETs." China Communications 14.9 (2017): 114-126.

[2] JeeHyeon Na, Yun Won Chung, Jaewook Shin, Sangho Lee, Sang-Ha Kim, "A Novel Routing Path Discovery and Data Delivery Scheme for Ubiquitous Internet Connectivity Based on Hierarchical Mobile AODV6 Networks", *Vehicular Technology Conference 2007. VTC2007-Spring. IEEE 65th*, pp. 61-65, 2007, ISSN 1550-2252.

[3] Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. *IEEE communications surveys & tutorials*, *15*(4), 2027-2045.

[4] Kavitha, P., Keerthana, C., Niroja, V., & Vivekanandhan, V. (2014). Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network. *International Journal of Communication and Computer Technologies*, *2*(02).

[5] Sun, Y., Han, Z., & Liu, K. R. (2008). Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine*, *46*(2), 112-119.

[6] Vasudeva, A., & Sood, M. (2012). Sybil attack on lowest id clustering algorithm in the mobile ad hoc network. *International Journal of Network Security & Its Applications*, *4*(5), 135.

[7] D. Sivakumar, B. Suseela and R. Varadharajan, "A survey of routing algorithms for MANET", *IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM -2012),* Nagapattinam, Tamil Nadu, 2012, pp. 625-640.

[8] Macker, J. (1999). Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations.

[9] Garg, N., & Mahapatra, R. P. (2009). Manet security issues. *IJCSNS*, *9*(8), 241.

[10] Douceur, J. R. (2002, March). The sybil attack. In *International Workshop on Peer-to-Peer Systems* (pp. 251-260). Springer, Berlin, Heidelberg.

[11] Piro, C., Shields, C., & Levine, B. N. (2006, August). Detecting the sybil attack in mobile ad hoc networks. In *Securecomm and Workshops, 2006* (pp. 1-11). IEEE.

[12] Abolhasan, M., Wysocki, T., & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. *Ad hoc networks*, *2*(1), 1-22.

[13] Marwaha, S., Tham, C. K., & Srinivasan, D. (2002, November). Mobile agents based routing protocol for mobile ad hoc networks. In *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE* (Vol. 1, pp. 163-167). IEEE.

[14] Alba, E., Dorronsoro, B., Luna, F., Nebro, A. J., Bouvry, P., & Hogie, L. (2007). A cellular multi-objective genetic algorithm for optimal broadcasting strategy in metropolitan MANETs. *Computer Communications*, *30*(4), 685-697.

[15] Kaaniche, H., & Kamoun, F. (2010). Mobility prediction in wireless ad hoc networks using neural networks. *arXiv preprint arXiv:1004.4610*.

[16] Ahmed Sherif, Maha Elsabrouty, Amin Shoukry,"A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET)", IEEE, pp: 346-352, 2013

[17] Bikramjeet Singh, Dasrari.S,C.R. Skitishn kumar,"Mitigating effects of Black hole Attack in Mobile Ad-hoc Networks: Military Perspective", 2nd IEEE International Conference on Engineering and Technology (ICETECH), 17th & 18th March 2016, Coimbatore, TN, India.

[18] 7. Paul, A., Sinha, S., & Pal, S. (2013, December). An efficient method to detect sybil attack using trust based model. In *Proc. of Int. Conf. on Advances in Computer Science, AETACS, Elsevier*.

[19] Pooja ,Dr.R.K.Chuhan, "An Assessment Based Approach To Detect Black Hole Attack In MANET", International Conference on Computing, Communication and Automation (ICCCA2015) ,IEEE2015.

[20] . Abbas, S., Merabti, M., Llewellyn-Jones, D., & Kifayat, K. (2013). Lightweight sybil attack detection in manets. *IEEE systems journal*, *7*(2), 236-248.

[21] Vimal Kumar a , Rakesh Kumar , " An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network",ELSEVIER , international Conference on Intelligent Computing, Communication & Convergence (ICCC-2014).

[22] Yibeltal Fantahun Alem,Y.C.Xeun , "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2010 IEEE.

[23] Siddharth Dhama, Sandeep Sharma, Mukul Saini, "Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks", 978-9-3805-4421-2/16/$31.00_c 2016 IEEE

[24] Z. Li and Y. Wu, "Smooth Mobility and Link Reliability-Based Optimized Link State Routing Scheme for MANETs," in *IEEE Communications Letters*, vol. 21, no. 7, pp. 1529-1532, July 2017.

[25] Y. Fang, Y. Zhou, X. Jiang and Y. Zhang, “Practical Performance of MANETs Under Limited Buffer and Packet Lifetime,” in *IEEE Systems Journal*, vol. 11, no. 2, pp. 995-1005, June 2017..

CITE AN ARTICLE

Pal, R. K., & Gupta, D., Dr. (2018). A REVIEW OF SECURE ROUTING PROTOCOLS FOR IPV6 BASED MOBILE AD-HOC NETWORKS (MANET). *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *7*(8), 245-250.