ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICACTRP 2017

International Conference on Advances in Computational Techniques and Research Practices

Noida Institute of Engineering & Technology, Greater Noida

Vol. 6, Special Issue 2, February 2017

A Literature Survey on Secure Gateway Discovery in MANET

Aanjey Mani Tripathi[1], Sarvpal Singh[1], Rahul Kumar Sharma[2]

Department of Computer Science and Engineering, Madan Mohan Malviya University of Technology, Gorakhpur[1]

NIET, Greater Noida, U.P[2]

Abstract: Mobile Adhoc network (MANET) is a collection of mobile node that can communicate with each other via radio or infra without any fixed infrastructure. MANET is a wireless network so to connect with internet any interface is needed that is called gateway which provide route to the internet. Due to dynamic topology packets are loss which degrade network operation. So, to achieved high throughput security scheme are applied on internet gateway which helps to out from adversarial environment. There is some security goal are discussed (confidentiality, integrity, authentication and non-repudiation) which enhanced adhoc network operation. In this paper, we survey on the gateway discovery scheme with security and without security based on various performance parameter like packet delivery ratio, end to end delay, routing overhead and throughput and then conclude which one is better.

Keywords: Mobile adhoc network(MANET) ; Secure and Non- secure Gateway discovery ; Attacks; Security goal ; Rabin signature scheme.

I. INTRODUCTION

Mobile adhoc networks (MANET) are a collection of terminals or wireless node that cannot have any fixed infrastructure [1,2]. Each mobile node in MANET can communicate and maintain data packets via wireless link over radio or infrared. Due to dynamic topology means sender node, receiver node and routing nodes all are mobile, his create a big issue in the design of adhoc network. With increase in wireless communication and portable devices such as laptop , PDAs and mobile phone which leads to people desired to connect with excellent and stable network at anytime and anywhere. The key point in MANET is to communicate between mobile nodes to the internet by scheme is called gateway discovery which act as a bridge between MN and internet.

Whenever mobile node willing to make connection before it search for an optimum gateway candidate by going through gateway selection scheme and then it connect with gateway. In wireless network some malicious nodes are present which makes interrupt in data forwarding operation to reach to the internet via gateway. The solution to the problem is to secure internet gateway by applying different security techniques like signature scheme. In this survey paper there are various gateway discovery approaches are taken either with security or without security that shows in which state of art its better. Some characteristics of MANET include distributed operation, open channel, malicious tempering, no central authority, dynamic topology and deletion, falsification of the routing information will raise it not work properly.

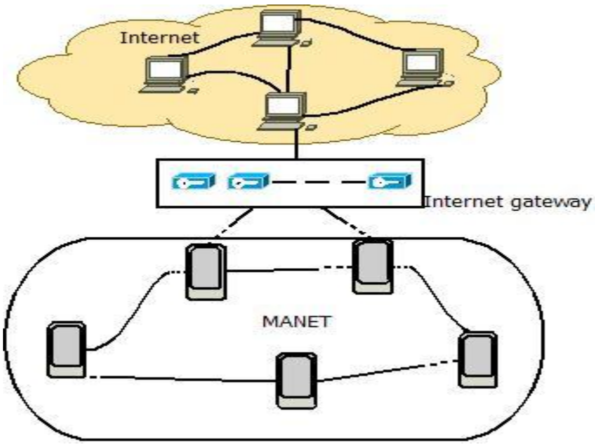


Fig.1. Hybrid network

A. Challenges-

- Dynamic Topology-In MANET all nodes are trust with each other .But due to dynamic topology, membership trust relationship are disturb if one node are detected as compromised node.
- Routing Overhead-In routing table some stale routes are generated because within network nodes often change their location, which leads to unnecessary routing overhead.
- Hidden terminal problem-It defined only the transmission range of the receiver but not the sender. Therefore at the receiver end collision of packet occur due to synchronous transmission of those nodes.

- Packet loss due to transmission error-Several factors such as hidden terminal problem ,uni -directional links, presence of interference and frequent path break due to mobility of nodes experiences a much higher packet loss.
- Mobility induced route changes-Route changes when frequent path break occur in an ongoing session due to movement of nodes in highly dynamic network topology.
- Battery constraint-The devices within network have restriction on the power source in order to preserve weight, size and portability of the devices.
- Security threats-As the wireless medium is prone to eavesdropping and adhoc network suitability is demonstrate through node association, MANET are intrinsically open to many security attacks.
- Limited bandwidth-Discover throughput after sum of noise and interference condition ,effect of multiple access and fading is always less than maximum radio transmission rates in wireless communication.

B. Application-

Some of well known application of MANET are given in table below-

- **Military battlefield-** Using common place network technology, the military can preserve an information between soldiers, military information headquarters and vehicles.
- **Collaborative work-** For an outside environment, the collaborative computing is more important than inside environment because people exchange and cooperate in an outside meeting.
- **Low level-** By using notebook computer in a temporary link multimedia network spreading of information among participant takes place.
- **Personal area network and Bluetooth-** It is a localized and short range network in which nodes are associated with a person. Bluetooth is a short-range MANET which is responsible for inter communication between several mobile devices such as mobile phone and laptop.
- **Commercial sector-** Adhoc can be used and emergency /rescue operation is performed during disaster like earthquake, flood and fire for relief.

The rest of the paper is follows as- Section II defines the routing protocol , Section III containg the gateway discovery approach, Related work on unsecure and secure gateway discovery in Section.IV ,Attacks are in Section ,Security goals describe in Section.VI , Section VII given Rabin signature scheme based on assymmetric cryptography technique. And the last Section VIII containing conclusion which conclude which approach gives better performance either non secure or secure.

II. ROUTING PROTOCOL

In a network ,due to congestion packets are dropped .So to overcome these situation numerous routing protocol are discussed which have different standards for routing packets to a correct destination .This protocol is used for finding routes from source to receiver which increases throughput, reduce end to end delay etc. There are three types of routing protocol i.e. ,proactive, reactive and hybrid routing protocol are given below-

A. Proactive routing protocol or Table driven-

As the name implies ,proactive periodically send routing information to other nodes in the network .For maintaining consistency it hold all the up to date information of the network which is used in finding optimal route from all other neighboring nodes .If node send routing information to other nodes and routes are already existed then without delay transmission of packet occur. Otherwise traffic packets are waiting in the queue until the route to that node is established . Adhoc network are location variant therefore table driven need many resources to keep the network reliable and up to date. Some of the proactive protocols are cluster head gateway switch routing (CGRS), hierarchical state routing(HSR) ,wireless routing protocol(WRP) [3] and DSDV (Destination Sequenced Distance Vector) [4].

B. Reactive routing protocol –

This protocol is used to established route when needed .It is also referred as On demand routing because route discovery approach is invoked when source node create a route before sending information to the destination. Once a route is discover then route maintenance process is maintained route until route are required very long or unreachable of route occur. Some of well known protocol of reactive is AODV(Adhoc on demand distance vector) [5], LMR(Label based multipath routing) ,LUNAR (Lightweight underway adhoc routing) and TORA(Temporally ordered routing algorithm) [6].

C. Hybrid routing protocol-

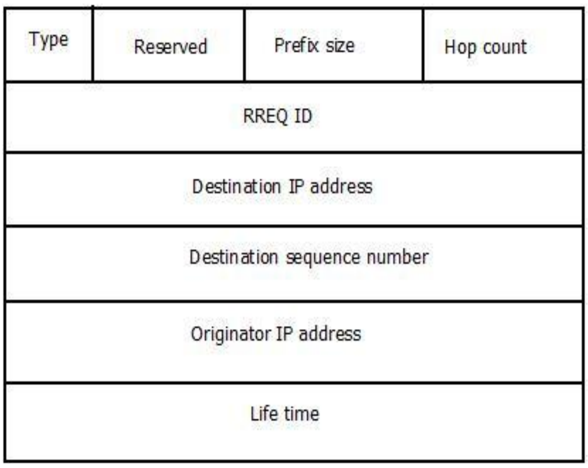
It is a combination of both proactive and reactive protocol and it take advantages of both. The protocol, ZRP (Zone routing protocol)[7,8] and HARP (Hybrid adhoc routing protocol) belongs to hybrid protocol.

III. GATEWAY DISCOVERY APPROACH

Gateway is the bridge defined between the wired network and the wireless network which provide service to the mobile node. There are four broadly classified approaches are present which is used to detect route for accessing the internet via gateway. MANET are infrastructureless so MN can identify the route to the gateway by following given approach-

A. Proactive gateway discovery-

In this approach gateway periodically broadcast GWADV message within MANET. The GWADV message is the extended version of RRER-I message and contain additional field of RREQ message that is RREQ-ID field. The mobile nodes are connected with gateway after receiving message and rebroadcasted GWADV message if original IP address and RREQ-ID field are match with GWADV message and do not lie within MANET. As shown in figure internet gateway send GWADV message periodically in MANET. The mobile node that willing for route are connected with gateway in figure MN1 are connected with gateway and then it rebroadcast GWADV message for another mobile nodes in MANET. In this way all four mobile nodes get connection and send packets to the desire node in the internet. It gives solution of duplicated address problem but flooding occur still by gateway advertisement message .The format of GWADV message are given in fig-



Type	Reserved	Prefix size	Hop count
RREQ ID			
Destination IP address			
Destination sequence number			
Originator IP address			
Life time			

Fig.2. Format of GWADV message

B. Reactive discovery approach-

Unlike proactive approach, Mobile nodes that need to search for route or modified existing route to the gateway then it use expanding search technique which helps in connection between adhoc network nodes and the internet .By using this technique source mobile node broadcasted RREQ-I message to the IP of combine gateway that is ALL-MANET-GW-MULTICAST address. To overcome duplicate address problem intermediate nodes helps in rebroadcast message after evaluating RREQ-ID field .When gateway receive message then it send RREP-I message to the requesting node in a unicast way .The gateway selection criteria is based on hop count .After selection gateway source node forward data packets to gateway and then from gateway it move to the destined node in internet. The figure below illustrate that MN1 are willing for internet connection then it broadcast gateway solicitation message to the internet gateway IP and wait for replying .

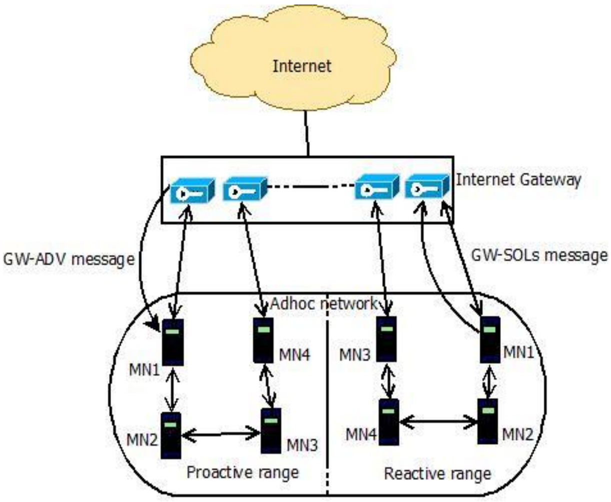
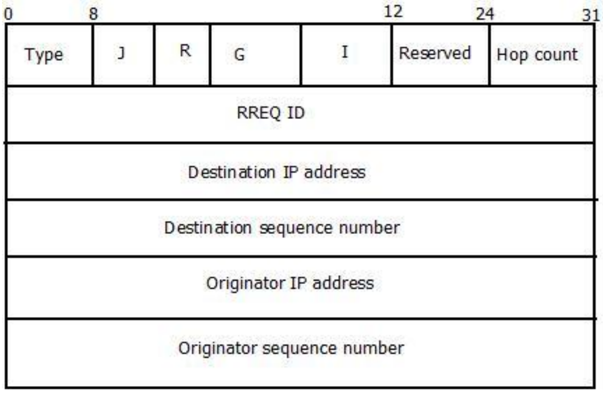


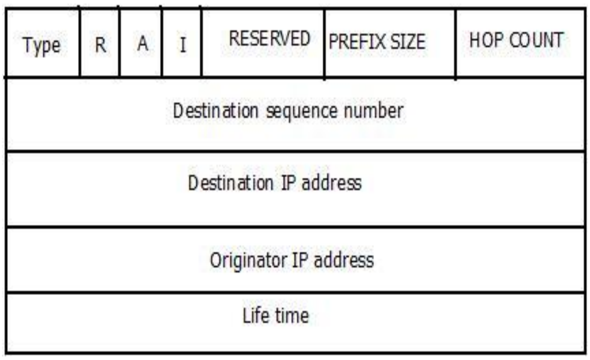
Fig.3. Proactive and Reactive discovery approach

Extended route request and route reply message-Extension is applied to AODV routing protocol for route discovery of other mobile nodes and gateway also. Standard routing protocol is designed in such a way that its not search for gateway ,therefore existing protocol are extended .As like normal route request and route reply its work ,but only one field is extra that is I-flag field used for global internet connection in both route request and reply field. The format of RREQ and RREP is given in fig.



0	8				12	24 31
Type	J	R	G	I	Reserved	Hop count
RREQ ID						
Destination IP address						
Destination sequence number						
Originator IP address						
Originator sequence number						

Fig.4. Extended RREQ message format



Type	R	A	I	RESERVED	PREFIX SIZE	HOP COUNT
Destination sequence number						
Destination IP address						
Originator IP address						
Life time						

Fig.5. Extended RREP message format

C. Hybrid discovery approach

This is a mixture of both approaches means at a certain time to live or we say that IGW range, inside a range proactive approach is work well but after range reactive approach work to discover information from IGW. This approach used both merits to balance delay and control overhead.

D. Adaptive gateway discovery approach

All the approaches in gateway discovery based on the TTL (time to live) GWADV message. This approach [9] is able to adopt the new environment by expanding the range of TTL due to which every mobile nodes update their own routing table .The scope of advertisement message has great impact in proactive and reactive gateway discovery and the operation also depend on network condition, dynamic node and the network traffic. When the TTL value reaches to zero then approach is reactive type and if value of TTL becoming to network diameter then associated scheme is completely proactive.

TTL=0 (reactive approach)

TTL= Network- diameter (proactive approach)

IV. RELATED WORK

Jonsson et al [10] proposed MIPMANET method that depend on AODV .The concept of tunneling and mobile IP is used for internet connectivity. When mobile node wants to connect with internet then it innitially registered with foreign agent then all the packets are tunneled in foreign agent and send to the destined node. MIPMANET avoid default route by tunneling and it permits coming node for switching between one foreign agent (current) to another this process is called handoff which happening by MIPMANET cell switching algorithm

E.M Building –Royer et al [11] proposed a proactive agent solicitation procedure which is used to discover AODV route and it register in mobile IP. This paper define mobile IP which is used by Adhoc network IPV4 with reactive routing protocol AODV. To avoid default route of destination node , it find F-RREP of FA which helps in making distinguished between different destination node location. This scheme takes more time for connection setup because innitially it check that destination node is not with range of MANET before FA can be used by MN

Ergen and puri et al [12] proposed extended solution of mobile IP means it provide internet connectivity in a local area architecture which is wireless.It define two protocol , one is MEWLANA-TD that belong to table driven routing protocol and used by DSDV and other is MEWLANA-RD that are route driven protocol and used by TBBR (Tree Based Bidirectional Routing) .The table in TBBR is formed by agent advertisement message and registration route request message and that is update at the time of renewal. When network operation downgrading then TBBR protocol is cost saving. For small size MANET means more internal traffic MEWLANA –TD is suitable and for large size MANET means less internal traffic MEWLANA-RD is appropriate for correct operation.

Ratanchandani et al [13] uses mobile IP and AODV in foreign agent to provide connection in MANET and the internet. Foreign agent fixed TTL (time to live) value upto certain number of hops. The node which are closer to FA can easily requested for route but when mobile nodes are far then node send solicitation message for connection..The intermediate node also permit to reply requesting node having cache information, agent advertisement and to eavesdrop in a unicast manner.

Wakikawa et al [14] shows how mobile node in MANET IPV6 environment are globally interconnected via internet gateway. This paper present both reactive and proactive approach. The proactive approach performed by broadcasting GWADV message periodically in adhoc network. The mobile node connect with gateway after receiving GWADV message .The GWADV message containing network prefix address ,address length and life time which configure mobile node with newly routable global address that depend on IPV6 NDP (Neighbor Discovery Protocol).Unlike proactive ,reactive approach need connection then mobile node actively send GWSOLs message to gateway.

M.Ghassemian et al [15] define AODV6 routing protocol implementation which used extra flag called as internet-global address resolution flag .The scheme is describe for efficient operation between mobile node and gateway .When mobile node need connectivity then it send gateway solicitation message to the gateway and wait for reply. The gateway response by sending IPV6 address and globally routable prefix by receiving this address from gateway MN binding update with HA and used this as a care of address.

Bin Xie and Anoop kumar et al [16] ,proposed a protocol minimal public based authentication which help in maintaining integrity and authentication .Each node having certificate authentication which can be refresh periodically to avoid malicious node.

Bok- Nyong park,Wenjum lee and Christian shin [17, 18] proposed a registration mechanism in foreign network and for authentication propose secret key are distributed in MANET and foreign network

Rafi U Zaman et al[19] specified load balancing routing protocol referred as Modified AODV and WLB-AODV .By using these protocol it proposed a load balancing scheme in two gateway which helps in connection MANET and the internet. The protocol WLB-AODV is more reliable and efficient then Modified AODV.

Xu Zhanyang ,Han Xia oxuan,Nanjing [20] proposed virtual structure for MANET called V-MANET. This scheme launched new gateway and delete previous gateway which are fixed for LAN operation before deletion neighboring nodes are exchanged information

Huilei and Charles E.Perkin et al [21] proposed integration of mobile IP routing and adhoc network routing which comes under proactive approach..Within MANET proactive routing protocol routed is used for routing which is update version of RIP(Routing Information Protocol).The aimed of integration is to permit foreign agent in wireless networking routing .Foreign agent behave as a default router among individual mobile node. If mobile node need route between adhoc network and foreign agent then update RIP transfer registration and advertisement message through multi hop path.

Rashween kaur salija and rajesh srivastava [22] proposed reactive routing protocol AODV that are modified to support interconnection between MANET and internet .There are various discovery approaches are needed to find route between mobile node and internet. The hybrid approach discover is seemed typical and challenging task. The network performance are determined by following metrics that are average end to end delay ,packet delivery fraction and normalized routing load..

Morli pandya and Ashish kr. Srivastava [23] proposed a two layer signature scheme on AODV routing protocol which aimed to improved network security therefore it using digital signature and secure hash function for the extended AODV routing protocol.

Mohammad Asrar Ahmed and Khaleel ur Rahman khan et al [24] proposed load aware ,gateway discovery security scheme and trust among nodes by authentication. To prevent mobile nodes from non-adversarial environment , adaptive load balancing scheme is used which enhanced network operation and gives high throughput.

Performance parameter-There are some parameters are given like packet delivery ratio, end to end delay ,routing overhead and throughput .On the basis of this parameter we can able to judge security/non-security related proposed protocol that which is better.

1. Packet delivery ratio(PDR) -It is the ratio between the number of packet send by sender to the total number of packet received by the receiver .The percentage is the measurement of PDR.
2. End to end delay-It is the overall time taken by the packet to sending from source to destination.
3. Throughput-It is defined as the number of message received in per unit time.
4. Routing overhead-It is the sum of the routing packet which are forwarding between source and destination.

V. ATTACKS IN MANET

Due to absence of central co-ordination , nodes in MANET are shared different wireless medium which affect or damaged the network activity because various attacks are present in the environment which dismiss the transmission of information. Therefore many security solution are defined to protect data from various form of attack which is a big task in adhoc network. These attack are split into various categories.

External attack-This attack belongs to the type where nodes are not defined within the logical network. The outside node tried to penetrate network region to establish its attack. Routes are congested by sending wrong routing information.

Internal attack-This class includes the nodes which are part of network but launched an attack is called compromised node which provide access to unauthorized user .The malicious node form a traffic while connecting with other network activities.

Passive attack-This type of attack collect all information in the network and then this information is used by active attack .The attacker retrieve all useful information and start dropping of packets .The security scheme used to avoid this types of attacker behaviour is confidentiality .

Active attack-This includes hijacking , sleep deprivation and jamming types attack in which attacker aim is to only disrupt communication between two entities by which unavailability occur when authorized access by user.

VI. SECURITY GOAL

Security [25] is an art which apply on data during transmission to protect it from unauthorized user. There are various attacks are present either people in outside or in inside. So to protect resources and information there are five pillars of security schemes are discussed in Adhoc routing protocol which are given below-

- Data Confidentiality-This policy assured that the sending information is only be read by intended recipient. It limiting the accessing of information up to authorized people only.
- Authentication-For genuine communication between two nodes authentication is needed which is used to verify a claim of identity. when sender send packets then on each packet public key signature is apply which is the intuitive solution for authentication. And for group authentication private key signature is used by each sender.
- Data Integrity-It is the high indicator of security, which defines the origin of data means receiver trust upon the genuine source that it’s not being altered or changed data to disrupt the communication.
- Availability-The purpose of information system is to serve people whenever they are need .It is the reliable way which provide available information to the user in a timely manner.
- Non-repudiation-When communication takes place then receiver have all burden to proof that the received information must be came from a valid sender. A mechanism is used which prove that the sending information is legitimate and both sender and receiver not able to deny falsely information.

Table: 1 Attacks in different layers

Attack	Layer	Attack type	Description
Passive		Eavesdropping	The attacker secretly listen all private conversation and find confidential information.
		Traffic analysis and monitoring	Attacker monitors the transmitted packet, and then derives important information by message interference.
Active	MAC Network	Jamming	Jamming is similar as DOS attacker that aimed is to prevent legitimate communication.
		Warm hole	There are two nodes connected by tunnel one is used for recording message and other is used for replay. These two-colliding node makes difficulty in packet transfer.
		Black hole	This attack followed denial of services attack. It disrupts routing Packet to reach at their Packet delivery rate is low.
		Byzantine	The compromised (intermediate) nodes formed routing loops that result in Down level the routing services.
		Routing attack	The attacker aimed to reduce Network operation by applying following techniques Routing table, routing overflow, poisoning and packet Replication, route cache Poisoning a brushing Attack.
		Power consumption	It is also called sleep deprivation attack in which attacker Trying to consume battery Life by continuously sending Packet and route request.
		IP spoofing	Misguide an attacker's true IP and takes benefit of illegitimate user.
		State pollution	As the name implies, pollution in the network occur because The malicious node replying Wrong parameter every time.
		Sybil attack	In peer to peer network, hacker trying to access a reputation System for unauthorized access.
		Fabrication	It happens when poisonous Node falsifies their own packet and mixed it in the net Work which violate Authenticity feature.
		Modification	This attack break integrity scheme by changing or modifying information in the Routing packet
	Transport	Session hijacking	Some standards are designed for network communication. Session token is one of standard which is used to set Connection, when token is Hacked then conversation is in unordered.
		SYN flooding	If attacker send SYN request Continuously to server then flooding occur which arises Unavailable of services to Authorized user
	Application	Repudiation	Without proof, it's difficult to Correctly identify the user. This attack defines capability of user Who deny for specific action.

Table.2. Secure/Non-Secure Gateway Discovery approach

Authors name	Gateway discovery technique	Routing protocol	Approach implemented	Mobile IP support	Security in adhoc network	Trust among nodes	Performance ratio without Security				Performance ratio with Security			
							Packet delivery ratio	End to end delay	Routing overhead	Throughput	Packet delivery ratio	End to end delay	Routing overhead	Throughput
Jonsson et al	Reactive	AODV	MIPMANET that integrate Mobile IP and FA care of address with internet	IPV4	NO	NO	High	low	Low	high	n/a	n/a	n/a	n/a

EM building-Royer et al	Proactive	AODV	Integrate mobile IP and AODV	YES	NO	NO	High	Low	Low	High	n/a	n/a	n/a	n/a
Ergen and Puri et al	Proactive	DSDV, TBBR	Mobile IP with DSDV and TBBR	IPV4	NO	NO	Optimum	Low	Eliminate	Extreme	n/a	n/a	n/a	n/a
M.Ghassemian et al	Proactive, Reactive	AODV6	Comparison between proactive and reactive approach	NO	NO	NO	Low	Average	High	Average	n/a	n/a	n/a	n/a
Rafi u Zaman et al	Adaptive	WLB-AODV	Address gateway discovery and load balance issue	NO	NO	NO	Exceed in sparse and dense environment	Good in thin environment	Low	Average	n/a	n/a	n/a	n/a
Xu Zhanyang, Han ziaet al	Reactive	AODV	Develop virtual MANET to connect with internet	NO	NO	NO	High	Low	Low	High	n/a	n/a	n/a	n/a
Rashween kaur salija et al	Reactive	AODV	Extend AODV for communication between MANET and internet	NO	NO	NO	Low	High	High	Low	n//a	n/a	n/a	n/a
Bin xie and Anoop kumar et al	Reactive	AODV	Modified minimal public based authentication protocol	YES	YES	YES	n/a	n/a	n/a	n/a	High	Low	Low	High
Bok Nyong Part et al	LAID	SDP	Registration mechanism to secure adhoc network and foreign agent	NO	YES	YES	n/a	n/a	n/a	n/a	High	Rare	Low	High
Morli Pandya et al	Reactive	AODV	Two-layer signature scheme on AODV	NO	YES	YES	n/a	n/a	n/a	n/a	High	Low	Low	High
M.Asrar Ahmad khan etal	Adaptive	AODV	Mutual trust and authentication among nodes	NO	YES	High	n/a	n/a	n/a	n/a	High	Decline	Decline	Increase

VII. CONCLUSION

Mobile adhoc network is leading in wireless technology. But due to no centralized structure, security become a big issue. Gateway is a heart of MANET. In the presence of malicious node attackers interrupt operation before reaching to the internet. Therefore many security scheme is applied on gateway that depend on trust among nodes. In this paper, we survey on gateway discovery with taking without security parameter and with security parameter that helps to find which of the two is better. This paper also revealed research for future direction. For providing more security in gateway discovery ,applied Rabin signature scheme which are based on asymmetric cryptography scheme.

REFERENCES

[1]. Attia, Radwa, RawyaRizk, and Hesham Arafat Ali. "Internet connectivity for mobile ad hoc network: a survey based study." Wireless networks 21, no. 7 (2015): 2369-2394.

[2]. Syarif, Abdusy, and RiriFitri Sari. "Performance analysis of AODV-UI routing protocol with energy consumption improvement under mobility models in hybrid ad hoc network." International Journal on Computer Science and Engineering 3, no. 7 (2011): 2904-2918.

[3]. S. Murphy and J. Garcia-Luna-Aceves, “A Routing Protocol for Packet Radio Networks”, Proceedings Of ACM Mobile Computing and Networking Conference, MOBICOM’95, Nov, 14-15, 1995.(wrp)

[4]. S. A. Ade& P.A.Tijare “Performance Comparison of AODV, DSDV, OLSR and DSR”, International Journal of Information Technology and Knowledge Management July-December 2010.(dsdv)

[5]. Mohammed Bouhorma, H. Bentaouit and A.Boudhir, “Performance Comparison of Ad-hoc Routing Protocols AODV and DSR “, 2009 IEEE.(aodv)

[6]. V. D. Park and M.S. Corson, “A highly adaptive distributed routing algorithm for mobile wireless networks”, http://www.ics.uci.edu/~atm/adhoc/paper-collection/corson adaptive-routing-infocom97.pdf

[7]. Z. J. Haas, “A New Routing Protocol for the Reconfigurable Wireless Networks”, http://www.ee.cornell.edu/~jaas/wnl.html, April 1, 2000.

[8]. Z. J Haas and M. R. Perlman, “The Zone Routing Protocol (ZRP) for Ad Hoc Networks,” IETF Internet draft, draft-ietf-manet-zone-zrp-01.txt, Feb, 1999.

[9]. Rakeshkumar, V. and Misra, M. An Efficient Mechanism forConnecting MANET and Internet through Complete AdaptiveGateway Discovery. In Proceedings of the First InternationalConference on Communication System Software and Middleware(COMSWARE2006). New Delhi, India, January 2006, 1-5.

[10]. U. Jonsson, F. Alriksson, T. Larsson, P. Johansson, a G.M. Maquire, “MIPMANET: Mobile IP for Mobile AdHoc Networks,” Proceedings of IEEE/ACM Workshop on Mobile and Ad Hoc Networking and Computing (MobiHoc 2000), Boston, MA USA, pp. 75-80, August 1999.

[11]. E.M. Belding-Royer, Y. Sun, C.E. Perkins, “Global Connectivity for IPv4 Mobile Ad Hoc Network, IETF Internet-Draft, draft-ietf-manet-globalv4-00.txt, November 2001.

[12]. E.M. Belding-Royer, Y. Sun, C.E. Perkins, “Global Connectivity for IPv4 Mobile Ad Hoc Network, IETF Internet-Draft, draft-ietf-manet-globalv4-00.txt, November 2001.

[13]. P. Ratanchandani, and R. Kravets, “A Hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks,” in Proceedings of the IEEE WCNC 2003, New Orleans, USA, vol. 3, pp. 1522-1527, March 2003.

[14]. Wakikawa R., Malinen J., Perkins C., Nilsson A., “Global Connectivity for IPv6 Mobile Ad Hoc Networks” In IETF Internet Draft 2003.

[15]. M. Ghassemian, H. Aghvami, "Comparing different handover schemes in IP based Micro-Mobility Protocols", Proceedings of IST Mobile & Wireless Telecommunications Summit 2002, pp 95-99, June 2002

16. Xie, B., Kumar, A.: A framework for Internet and MANET Security. In: IEEE Symposium on Computers and Communications (ISCC) (June 2004).

17. B. Park and W. Lee, "ISMANET: A Secure Routing Protocol using Identity-based Signcryption Scheme for Mobile Ad-hoc Networks," IEICE Transaction on Communications,Vol. E88-B, No. 6, June 2005.

18. B. Park, W. Lee, C. Lee, J. Hong, and J. Kim, \LAID: Load-Adaptive Internet Gateway Discovery for Ubiquitous Wireless Internet Access Networks," Proceed-ings of the International Conference on Information Networking (ICOIN) 2006. January 2006.

19. Rafi U Zaman, Khaleel Ur Rahman Khan, M.A.Razzaq and A. Venugopal Reddy, “A Simulation Based Comparison of Gateway Load Balancing Strategies in Integrated Internet-MANET”, 17th International Conference on Advanced Computing and Communication (ADCOM’09) 14-17 December 2009. IISC Bangalore, Published by IEEE Computer Society, pages: 270 – 272.

20. Xu Zhanyang, Han Xiaoxuan and Zhang, “A simplified scheme of internet Gateway Discovery and Selection for MANET’’, International conference on Wireless communication, Networking and Mobile computing ,IEEE, Sep-2009.

21. H. Lei, C. E. Perkins. “Ad Hoc Networking with Mobile IP”, in the Proceedings of Second European Personal Mobile Communications Conference (EPMCC’97), Bonn, Germany, September 30 – October 2, 1997.

22. Rashween kaur and Rajesh shrivastava, ‘‘A scenario based approach for Gateway Discovery using MANET routing protocol ’’,ICCCI International Conference on Computer and Informatics, Jan-12 , 2012.

23. Morli Pandya and Ashish kr.Srivastava ,” Improvising Performance with Security of AODV Routing for MANET,” IJCA International Journal of Computer Application , VOL 78 NO. 11, Sep. 2013

24. Mohammad Asrar Ahmad, Khaleel Ur Rahman Khan, “Trust Based Secure Gateway Discovery Mechanism for Integrated Internet and MANET”, ICDCIT 2013, LNCS 7753,Springer-Verlag Berlin Heidelberg , pp. 103-114.

25. Frank Stajano and Ross Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In 7th International Security Protocols Workshop, Cambridge, UK, April 1999.

26. William Stallings. Cryptography and Network Security principles and practices. Pearson Education Inc, third edition edition, 2003.

27. Rabin, M.O. (1978). “Digitalized signatures.” Foundationsof Secure Computation, eds. R. Lipton andR. De Millo. Academic Press, New York, 155–166.

28. Digitalized signatures and public key functions as intractable as factorization”, MIT/LCS/TR-212, MIT Laboratory for Computer

29. Coron Jean-S´ebastien (2000). “On the exact security of full domain hash.” Advances in Cryptology—CRYPTO 2000, Lecture Notes in Computer Science,vol. 1880, ed. M. Bellare. Springer-Verlag, Berlin,229–35

30. Bellare,M. and P. Rogaway (1995). “Optimal asymmetric encryption—how to encrypt with RSA.” Advances in Cryptography—EUROCRYPT’94, Lecture Notes in Computer Science, vol. 950, ed. A.De Santis. Springer-Verlag, Berlin, 92–111.

31. Mihir Bellare and Phillip Rogaway (1996). “The exact security of digital signatures: How to sign with RSA and Rabin.” Advances in Cryptology—EUROCRYPT’96, Lecture Notes in Computer Science, vol. 1070, ed. U. Maurer. Springer-Verlag,Berlin, 399–416.

32. Bucher Gruppe, Asymmetrisches Verschlusselungsverfahren: Rsa-Kryptosystem, Asymmetrisches Kryptosystem, Rabin-Kryptosystem, Elgamal-Kryptosyste

33. Wenbo Mao, Modern Cryptography theory and practises