Volume 2, No. 6, June 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARICLE
Available Online at www.jgrcs.info

PREVENTION AND REACTION BASED SECURE ROUTING IN MANETS

Ajay Jangra[1*], Shalini[2], Nitin Goel[3]
[1,2,3]CSE Department, UIET, Kurukshetra University, Kurukshetra, INDIA

er_jangra@yahoo.co.in[1], shalinisingroha@gmail.com[2], goelnitin0887@gmail.com[3]

Abstract: Mobile Ad hoc network can be set up anywhere, anytime without any predefined network infrastructure. Due to the infrastructure-less property, it becomes difficult to make use of the existing routing protocols for network services and it arises to a number of challenges in ensuring the security of the communication. Most of the ad hoc routing protocols that address security issues rely on trust relationships to route packets among participating nodes. These papers deal and analyze threats faced by ad hoc environments and provide corresponding security mechanisms. In this paper we present respective strengths and threats of the existing routing protocols and suggest an appropriate framework that can provide a trustful solution.

Keywords: Mobile Ad-hoc Networks (MANETs), multi-hoping, multicasting, Secure Routing, Security attacks.

INTRODUCTION

MANET is a collection of nodes, which organize itself without any central coordinator, and nodes move freely in the network. They may enter or exist the network without any restrictions. Therefore, wireless ad hoc network's topologies are dynamic and it is costly to maintain. So, wireless channels make message transmission and routing more challenging [1]. Nodes of adhoc networks can function as routers that discover and keep routes to other nodes as well as end-users. Nodes in wireless adhoc networks have limited resources i.e. bandwidth, battery power and CPU power. Furthermore in this situation, a trustworthy environment is main issue in wireless ad hoc routing protocol [2].

Ordinary networks work in different situation. They equipped with fixed topology of a large number of nodes, which are preconfigured, the connection. In these networks, routing service is provided certain organizations with authority and users trust them to pass the messages. In ordinary networks, entities are powerful and enough computational ability and easily Public Key Infrastructure (PKI) can be constructed. So, the replacement of common routing protocols is not possible and securing infrastructure to MANET because of above reasons. Therefore, trust is introduced to solve this problem and used in many present protocols for ad hoc networks to enhance security [2]. Ad hoc routing protocols categorized in to two types: -

Table-driven Routing Protocols: - It is also known as proactive routing protocols. These protocols maintain routing information consistent and up-to-date the routes by broadcasting update message. Some examples of these protocols include DSDV, OLSR and WRP.

On-Demand Routing Protocols: - It is also known as reactive protocols. In these protocols route discovery is performed when communication between hosts of a mobile network is required. Examples of reactive routing protocols include AODV, DSR and TORA [3].
Because of information-exchanged overhead, especially in volatile environment, proactive routing protocols are not suitable for mobile ad hoc networks [2].

CLASSIFICATION OF ATTACKS

In ad hoc networks attacks can be classified on basis of their origin, either external or internal. Where *the parties that are not part of the network launch External Attack*. These attackers are not necessarily disconnected from the network and internal *attacks* are sourced from inside a particular network. A network which contains these internal attackers' nodes is more vulnerable because a malicious node inside a network is already past the basic defense lines of a network, therefore the malicious activity is difficult detect and curtail [3].

The attacks on network can be defined as follows:-

(i) *Passive Attacks*: - These attacks does not affect the operation of the protocol, instead it tries to discover valuable information by listening to traffic.

(ii) *Active attacks*: - In these attacks a node proactively searches for flaws in the network. These attacks try to disrupt the topology of the network by breaking existing paths between network nodes [3].

CHALLENGES TO AD HOC ROUTING

Existing MANET routing protocols faces many problems, such as security and performance. These are describing as follows:-

(i) *Denial of service (DOS)*:- In this attack, a malicious node become the bottleneck for paths that are passing through it, by denying service provided to those paths. In DOS, a particular node that contain single or multiple paths passing through it may stop forwarding packets and still maintaining its presence in the network, therefore behave as a sink for data in the network.

(ii) *Black Hole*: - In black hole attack malicious node replies to every RREQ by falsely claiming that it contain a fresh enough route to the destination. Hence all the traffic of the network is redirected to that malicious node which then dumps them all [4].

(iii) *Rushing*: - It results in denial-of-service when used against all previous on-demand ad hoc networks routing protocol. In this, attacker relays received route request without any change as soon as possible, by suppressing any later legitimate route request [5].

(iv) *Wormhole*: - These attacks are hard to detect because the path that is used to pass on information is not part of the actual network. In this, a malicious node uses external path in the network to route messages to other node at other location [6].

(v) *Selfish*: - As nodes in MANET have limited resources, especially battery power and bandwidth. Hence some nodes deny to forward or selectively forwarding the packets from other nodes to save its resources.

In general following types of misbehavior can be shown by malicious nodes:-

- First is No Forwarding (i.e. of neither control messages nor data).
- Second is unusual traffic attraction (i.e. advertises more very good routes or advertises routes very fast; hence they are deemed good routes).
- Third is Deflecting traffic in order not to be used on a route.
- Fourth is lack of error messages; however an error has been observed.
- Fifth is Route solving (i.e. rerouting to avoid a broken link), however no error has been observed.
- Sixth is fabricating of error messages, however no error has been observed.

Without any appropriate countermeasures, many simulations that dramatically decrease the network performance have showed the effects of misbehavior. So based on the proportion of misbehaved nodes and their specific strategies network throughput can be degraded, packet loss increases, nodes can be denied services and the network can be portioned [1].

CLASSIFICATION OF SECURE AD HOC NETWORKS TECHNIQUES

They are basically two approaches used these days to provide solutions to the security issues in ad hoc networks.

- Prevention Techniques in MANETs
- Detection and Reaction Techniques in MANETs

Prevention mechanism cannot provide guarantee to complete cooperation among nodes in the network. These mechanisms require encryption techniques to provide authentication, confidentiality, integrity and non-repudiation of routing information. However existing preventive approaches, some approaches some use symmetric algorithms, some use asymmetric algorithm; while the others use on-way hashing, individual having different trade-offs and goals. On the other side, detection approaches specifies solutions that try to identify clues of any unauthorized activity in the network and take appropriate action against such nodes [7].

PREVENTION USING ASYMMETRIC CRYPTOGRAPHY IN MANETS

These asymmetric cryptography techniques give the underlined basic methodology of operation of protocols under this category. A secure wired network is needed to distribute public keys on digital certificates in the ad hoc networks. In mathematical terms, a network with n nodes would demands n public keys stored in the network. Two protocols SAODV and ARAN are defined in this category.

SECURE AD HOC ON-DEMAND DISTANCE VECTOR ROUTING (SAODV)

It is an extension to AODV routing protocol. SAODV functionality work under in security the AODV protocol by authenticating the unchangeable fields of the routing messages using digital signatures. This protocol gives an end-to-end authentication and node-to-node verification of the messages. It is a simple process. The source node digitally signs the route request packet (RREQ) and broadcasts it to its neighbors. When any intermediate node receives a route request message, it first verifies the signature before creating or updating a reverse route to its predecessor. Then it stores or updates the route only if the signature is verified. Same procedure is followed for the route reply (RREP) packet. As there is an optimization, intermediate nodes can also reply with route reply messages if they have a “fresh enough” route to destination. Although the intermediate node will have to digitally sign the RREP message as it came from destination, it uses the double signature extension described is SAODV protocol.
Issue: - There is only one mutable field in this protocol is the hop-count value. To prevent from wormhole attacks this protocol determines a hash of the hop count field [8].

AUTHENTICATED ROUTING FOR AD HOC NETWORKS (ARAN)

It is an on-demand routing protocol that makes use of cryptographic certificates to provide routing security. This is a preliminary certification process that uses a route instantiation process that guarantees end-to-end authentication.

ARAN protocol wants the use of a trusted certificate server T, whose public key is known to all the nodes in the network. In this protocol end-to-end authentication is achieved by the source by having it check that the intended designation was reached. In the process of ARAN, the source trusts the destination to select the return path. In this protocol, the source starts route instantiation by broadcasting a Route discovery packet (RDP) that is digitally signed by the source. Then each intermediate node checks the integrity of the packet received by valid signature. First of all, the first intermediate node appends its

own signature encapsulated over the signed packet that it gets from the source. The other entire subsequent intermediate node deletes the signature of their predecessor, verify it and then append their signature to the packet. The Route discovery packet consists of a nonce and timestamp to protect reply attacks and to detect looping. Similarly, each node along the destination to source path signs the REP and modifies its own certificate before forwarding the REP to the next hop. It does not protect nodes from advertising longer routes.

Issue: - Major issue of ARAN protocol is the requirement of a certificate server i.e. the integrity of that server is necessary. This is by although only a design issue and as it is intended for securing communication over a managed-open-environment, it shouldn't be considered a big issue [9].

These two protocols, SAODV & ARN do not address wormhole attacks. ARAN provides both node-to-node and end-to-end authentication while SAODV provide only end-to-end authentication.

PREVENTION USING SYMMETRIC CRYPTOGRAPHY

To avoid attacks on routing protocols we use symmetric cryptographic techniques. In this symmetric keys are pre-negotiated via a secured wired connection. By mathematical approach it provide that a network within 'n' nodes would require n* (n+1)/2 pair wise key store in the network. Two protocols are defined in this category. These are SAR and SRP.

SECURITY –AWARE AD HOC ROUTING (SAR)

This protocol use traditional symmetric key encryption in order to provide a higher level of security in mobile ad hoc networks.
To make secure routing decision; this protocol makes use of trust levels. However, existing routing protocols find out the shortest path between two nodes. This protocol cans also fid out a path with desired security attributes. The different trust levels are implemented by using shared symmetric keys. For a particular node to forward or receive a packet first of all it has to decrypt it and then it needs the requested key. Any nodes not on requested key and it can not forward or read the packets. Here each node sending a packet decides the trust level needed by every node that will send further the packet to its final destination.
Issue: - Here still a lot of security issues present that are still open for attacks such as:-

- This protocol is nothing is done to protect intervention of a possibility malicious node from being used for routing, as long as they have the required key.
- Second is that, if any malicious node somehow extracts the required key the protocol has no further security measure to protect against the attacker from halting the entire network for a moment [9].

SECURE ROUTING PROTOCOL (SRP)

Secure Routing protocol is another protocol that can be applied to any of the most commonly used protocols today. The basic process of SRP is to set up a SA (Security Association) between the source and the destination node.
Security Association is a secret key scheme used to preserve the integrity in the routing information. Security association is usually set up by fixing a shared key based on the other party's public key and then the key can be used to encrypt and decrypt the messages. It is required that the routing path is always sent along with the packets, encrypted though. These all features are achieved with low computational cost and bit overhead. This protocol is partially protect to IP spoofing and implements partial caching without any compromising security in the network. More than single Route Request (RREQ) packet reaches the destination through different routes. The destination calculates MAC covering the RREP contents and after that returns the packet to the source over the reverse route accumulates in the respective Route request (RREQ) packet. The destination send responds to many route request packets to provide the source with as a diverse topology picture as possible.
Issue: - In this protocol no defense against the "invisible node" attack that puts itself somewhere along the message path without adding itself to the path, so causes potentially more problems as far as routing goes [7].

PREVENTION USING ONE-WAY HASH CHAINS

This category classifies a one-way hash chain to prevent from attacks on routing protocols. This type of category prevent modification of routing information
such as metric, sequence number and source route. In this category two protocols are there. These are SEAD and Ariadne.

SECURE EFFICIENT AD HOC DISTANCE VECTOR (SEAD)

The main motive of the protocol is to avoid any malicious node from falsely advertising a better route or if it is received from the source then tamper the sequence no. in the packet. This protocol implements features to prevent modification of routing information such as sequence no. , metric and source route. This protocol uses a one-way hash chains for authenticating the metric and the sequence number. Every node creates a one –way hash chain and uses the elements in-group of 'm'; here m is the diameter of the network for each sequence number. Each single node uses a specific single upcoming element from its hash chain in each routing update that it transmits about itself and upper bound of the network represented by (m-1).

In SEAD, an entry is authenticated by using the sequence number in that entry to find out a contiguous group of m elements from that destination nodes hash chain, one element of which must be used to authenticate that routing update. This one-way nature of hash chains protects any node from advertising a route with a larger sequence no. than a source's sequence no. To remove routing loops the source of each routing updates message must be authenticated [10].

ARIADNE

This protocol relies on highly efficient symmetric cryptography. First of all this protocol discusses the use of a broadcast authentication protocol named as TESLA because of the reason that its efficiency and it requires low synchronization time rather than the high key setup overhead of using pair-wise shared key. The design of Ariadne contains 3 steps-

(i) *Authentication of RREQ by target-* In the first step, to convince the target of the legitimacy of every field in a RREQ, the initiator contains a MANC computed with a shared key over a timestamp.
(ii) *Mechanisms for authenticating data in RREQ and RREP-* This allow the initiator to authenticate each individual node in the node list of RREP. In the node list of the RREQ, the target in authenticate each node so that it will return Route Reply (RREP) only along paths that contain legitimate nodes.

Per-hop hashing Technique- Here a one-way hash function is used to avoid a node from being cut from the node list in the RREQ message. The source begins the hash chain to a MAC with a key shared between the source and target. When any intermediate node receives the request, it joins its identifier to the hash chain and rehashes it. Then the target verifies each hop of the path by differentiate the received hash and computed hash of the MAC. To change or remove a previous hop, the attacker demands to be able to negate the one way hash function, which has been proved computationally infeasible.

(iii) *Issue: -* It does not prevent nodes from advertising longer routes. It is not suitable in resource-constrained mobile ad hoc networks [11].

DETECTION AND REACTION TECHNIQUES IN MANETS

Detection defines solutions that attempt to find out clues of any malicious activity in the network and take punitive actions against such node. All protocols that are designed in this category able to detect malicious activates and react to the threat as required. The protocol lies under this category are Byzantine, Confidant, Core and a protocol that uses Reputation base Schemes.

BYZANTINE FAILURES

It defines as on demand routing protocol that constitutes detection mechanism in to its algorithm and attempts to survive under an adversarial network failures which contain modification/fabrication of packets, dropping packets, among others, caused by selfish or malicious nodes, collectively known as Byzantine failures.
This includes three phases- link weight management, Route Discovery with fault avoidance and Byzantine Fault Detection [7].

COLLABORATIVE REPUTATION MECHANISM (CORE)

It suggests a generic mechanism to stimulate node cooperation based on a collaborative monitoring technique. This can be integrated with any network and application layer function that can contain packet forwarding, route discovery network management, location management. It proposes a reputation based detection framework to handle selfish behavior of nodes. All the services available from the network, such as forwarding, are behaved as functions and reputation is calculated for each such function.

This defines three types of reputations- subjective, indirect and functional. Every node maintains a watchdog component and a reputation table for each function with entries for other nodes in the network.

(i) *Subjective Reputation-* It is a reputation value, which is locally estimated, based on direct observation. In direct observation, a node monitors the behavior of other nodes usually in one-hop to see if it works well.
(ii) *Indirect Reputation-* It is a second –hand reputation information that is established by other node. Acceptance or rejection of this information is based on the trust level of the sender node.
(iii) *Functional Reputation-* It is related to a certain function, where each function is given a weight as to its importance.
(iv) Based on all these factors that discussed above, a persistent non-cooperative behavior by any node will tend to its exclusion from the network [12].

COOPERATION OF NODES: FAIRNESS IN DYNAMIC AD HOC NETWORK (CONFIDANT)

Its motive is to detect and isolate misbehaving nodes in ad hoc network, then making it unattractive to deny cooperation and participation. Trust relationships and routing decisions are building based on experienced, prediction, or reported routing and forwarding behavior of other nodes. CONFIDANT protocol has been described using DSR (Dynamic Source Routing) in the network layer.

Each individual node Contains 4 components:-
(i) *Monitor-* It is equivalent to a "neighbor watch", in which nodes locally monitor deviating behavior.
(ii) Trust manager- Trust manager is responsible for calculating trust levels of nodes and dealing with an all-incoming and outgoing alarm messages.
(iii) Reputation system- This system manages a table consisting of entries of nodes and their corresponding ratings. The rating is changed if there present sufficient evidence of uncooperative node behavior that has occurred sufficiently many times to rule out coincidences.
(iv) Path Manager- Path manager manages all path information. That is adds, delets or updates paths according to the feedback it gets from the reputation system [12].

PROTOCOL USING REPUTATION BASED SCHEMES: COSR

It stands for Cooperative On-demands secure Route. It is a novel secure route protocol against the malicious and selfish behaviors and it makes all nodes more cooperative. It

measures node reputation (NR), Route reputation (RR) by contribution, Capability of Forwarding (CoF) and recommendation upon DSR (Dynamic Source Routing) and it uses Route reputation (RR) to balance load to avoid hotpoint [13].

In this protocol, node's reputation depends on the information from physical layer, and node's CoF, history action and recommendations can compute this. Basically this protocol can be divided in to five parts. These are explained as follows:-

Monitor- It includes three modules. These are neighbor monitor, data relay monitor and CoF monitor. Neighbor monitor is used to monitor neighbors in its radio range and perfectly maintain neighbor list. Data relay monitor requires MAC layer that is worked in a promiscuous mode. CoF would gather information about capability of forwarding from physical layer and MAC layer. It includes node's bandwidth, mobility status, interface state and power.

Statistics- It is responsible for providing data about neighbor's history behavior. This statistics consists of the number of the number of requested and forwarded protocol. STATISTICS number of requested and forwarded protocol messages and data packets. *Reputation model*- This model is the core module COSR. This is used to calculate node's reputation and also integrate route reputation relying on the data from MONITOR and STATSTICS.

Reputation Protocol: - It defines reputation discovery in the MANET. This protocol clings with routing protocol.

Routing Protocol- This is an extension of DSR by reputation model. This protocol uses NR and RR to select the best route path rather than path length [13].

Attacking	ARAN	SAODV	SRP	SEAD	Ariadne	CORE	CONFIDANT	COSR
Denail of Service Attack	Possible	Not Possible	Possible	Possible	Possible	Not Possible	Not Possible	Possible
Blackhole Attack	Not Possible	Not Possible	Not Possible	Not Possible	Not Possible	Possible	Possible	Possible
Rushing-Attack	Possible	Not Possible	Possible	Not Possible	Can be Solved with improvement	Not Possible	Not Possible	Can be Solved with improvement
Wormhole-Attack	Not possible	Not Possible	Not Possible	Not Possible	Can be Solved with improvement	Not Possible	Not Possible	Can be Solved with improvement
Selfish Attack	Not Possible	Not Possible	Not Possible	Not Possible	Not Possible	Possible	Possible	Possible

Comparison table of Secure Routing Protocols in ad hoc networks

CONCLUSION

MNAET works in infrastructure-less mode, which also provides a special invitation to attackers and vulnerability/security threats. Beyond proper security it is possible to gain many advantages by malicious behavior. So, by diverting the traffic towards from a node, no forwarding at all, incorrect forwarding, and other non-cooperative behavior, nodes can attack to the network. This paper deals with the various routing and forwarding attacks. We have also discussed prevention and detection techniques that were choose to give security in Ad hoc networks. We have also compares some security protocols in this paper.

REFERENCES

[1]. E.Venkat Reddy, " Trustworthy Robust Routing Protocol for Mobile Ad hoc Network", Amina Institute of Technology, Hyderabad, Andhra Pradesh-India, Published in E. Venkat reddy/ International Journal Of Engineering Science and Technology Vol.2 (2), 2010,77-86.

[2]. K.Seshadri Ramana, Dr. A.A.Chari, Prof. N.Kasiviswanth, "Trust Based Security Routing in Mobile Ad hoc Networks", Kurnool-518007, A.P., India. Published in K.Seshadri Ramana et.al./ (IJCSE) International Journal on Computer Science and engineering, Vol. 02, No. 02, 2010, 259-263.

[3]. Birinder Singh Sarao, Ashish Jolly and kamaljeet Kaur, "Mobile ad hoc Networks (MANETs) Routing Protocols", Mata Gujri College, Fategarh Sahib, Punjabi University.

[4]. Santhosh Krishna B.V, Mrs. Vallikannu A.L, " Detecting Malicious Nodes For Secure Routing in MANETs Using Reputation Based Mechanism", Published in International of Scientific & Engineering Research, Volume 1, Issue 3, December 2010.

[5]. Y.C.Hu,A. Perrig and D.B Johnson, "Rushing attacks and defense in Wireless ad hoc network routing protocols,", in proceddings of the ACM workshop on Wireless Security, pp. 172-194, ACM, September 2003.

[6]. Y.C. Hu, A. Perrig and D.B. Johnson, "Packets leashes: a defense against wormhole attacks in Wireless networks", in proceddings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Soieties, vol. 3, pp. 1976-1986, San Francisco, Calif, USA, March-April 2003.

[7]. C. Sreedhar,Dr.S.Madhusudhana Verma, Prof.N.Kasiviswanath, " A Survey on Security Issues in Wireless Ad hoc network Routing Protocols", Kurnool, Andhra Pradesh, India, Published in C.Sreedhar et.al. / (IJCSE) International Jounal on Computer Science and Engineering.

[8]. Manel Guerrero Zapata, " Secure Ad hoc On-Demand Distance Vector (SAODV) Routing INTERNET-DRAFT draft-guerreo-manet-sadodv-00.txt,August 2002. Published in the IETF MANET Mailing list October 8th 2001.

[9] S.Yi, P.NAldurg and R. Kravets Security –Aware Ad Hoc routing for Wireless Networks The Second ACM Symposium on Mobile Ad Hoc Networking & Computing, 2201. (Another version Security Aware Ad hoc Routing Protocol For Wireless Networks Report , August 2001.

[10]. Yih-Chun Hu, David B. Johnson and Adrian Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications, pp. 3-13, IEEE, Calicoon, NY, June2002.

[11]. Yih-Chun HU, Adrian Perrig, David B.Johnson, " ARIADNE: A Secure On-Demand Routing Protocol for Ad Hoc networks, MobiCOm 2002, September 23-28, 2002, Atlanta, Georgia, USA.

[12]. Jiangyi Hu and Mike Burmester, "Cooperation in Mobile Ad Hoc Networks", Florida State University,Tallahassee,USA, Springer- Verlag London Limited 2009.

[13]. Fei Wang, Furong Wang, Benxiong Huang and Laurence T.Yang, " Research Article COSR: A Reputation-Based Secure Route Protocol in MANET", Published in Hindawi Publishing Corporation, EURASIP Journal on Wireless Communications and Networking, Volume 2010, Article ID 258935, 10 Pages