Vol 2 Issue 11 May 2013

Impact Factor : 0.1870

ISSN No :2231-5063

Monthly Multidisciplinary Research Journal

GoldenResearch Thoughts

IMPACT FACTOR : 0.2105

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial Board readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.net

Golden Research Thoughts
Volume 2, Issue. 11, May. 2013
ISSN:-2231-5063
Available online at www.aygrt.isrj.net

ORIGINAL ARTICLE

A DETAILED STUDY ON INCREASING ENERGY EFFICIENT OF AODV IN MOBILE ADHOC NETWORK

NIRAJ THAKOR AND ROHIT SRIVASTAVA

Student, M.E. (CSE)
Assistant Professor, CSE Department
Parul Institute of Engineering &Technology

Abstract:

Ad hoc networking allows portable mobile devices to establish communication path without having any central infrastructure. Since there is no central infrastructure and the mobile devices are moving randomly, gives rise to various kinds of problems, such as routing and security.In this survey I am going to consider the problem of routing. Routing is one of the key issues in MANETs because of highly dynamic and distributed nature of nodes. Especially energy efficient routing is most important because all the nodes are battery powered. Failure of one node may affect the entire network. If a node runs out of energy the probability of network partitioning will be increased. Since every mobile node has limited power supply, energy depletion is become one of the main threats to the lifetime of the ad hoc network. So routing in MANET should be in such a way that it will use the remaining battery power in an efficient way to increase the life time of the network.

KEYWORDS:

Ad hoc network, portable mobile devices,central infrastructure, routing, security,energy efficient routing

INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a set of mobile nodes that perform basic networking functions like packet forwarding, routing, and service discovery without the need of an established infrastructure. All the nodes of an ad hoc network depend on each another in forwarding a packet from source to its destination, due to the limited transmission range of each mobile node's wireless transmissions. There is no centralized administration in ad hoc network. It guarantees that the network will not stop functioning just because one of the mobile nodes moves out of the range of the others. As nodes wish, they should be able to enter and leave the network. Multiple intermediate hops are generally needed to reach other nodes, due to the limited range of the nodes. Each and every node in an ad hoc network must be keen to forward packets for other nodes. This way, every node performs role of both, a host and a router. The topology of ad hoc networks is dynamic and changes with time as nodes move join or leave the ad hoc network. This unsteadiness of topology needs a routing protocol to run on each node to create and maintain routes among the nodes.

In this paper I am going to present a novel security scheme which integrates digital signature and hash chain mechanism to protect the AODV routing protocol that is capable of defending itself against both malicious and unauthenticated nodes with marginal performance difference and energy efficiency. The proposed security scheme is also planned to simulate on Network Simulator 2 (NS2).

Title : A DETAILED STUDY ON INCREASING ENERGY EFFICIENT OF AODV IN MOBILE ADHOC NETWORK
Source:Golden Research Thoughts [2231-5063]NIRAJ THAKOR AND ROHIT SRIVASTAVA yr:2013 vol:2 iss:11
.

2.BACKGROUND THEORY

2.1 OVERVIEW OF MOBILE AD HOC NETWORK

A Mobile Ad Hoc Network (MANET) [1] is a set of mobile nodes that perform basic networking functions like packet forwarding, routing, and service discovery without the need of an established infrastructure. All the nodes of an ad hoc network depend on each another in forwarding a packet from source to its destination, due to the limited transmission range of each mobile node's wireless transmissions. There is no centralized administration in ad hoc network. It guarantees that the network will not stop functioning just because one of the mobile nodes moves out of the range of the others. As nodes wish, they should be able to enter and leave the network. Multiple intermediate hops are generally needed to reach other nodes, due to the limited range of the nodes. Each and every node in an ad hoc network must be keen to forward packets for other nodes. This way, every node performs role of both, a host and a router. The topology of ad hoc networks is dynamic and changes with time as nodes move join or leave the ad hoc network. This unsteadiness of topology needs a routing protocol to run on each node to create and maintain routes among the nodes.

2.2 MOBILE AD HOC NETWORKS' CHARACTERISTICS AND CHALLENGES

MANETs have several major characteristics and challenges. They are as follows[6]:

Dynamic topologies: Nodes are allowed to move randomly. Thus, the network topology may change randomly and rapidly at unpredictable times.
Bandwidth-constrained, variable capacity links: Wireless links have significantly lower capacity than their hardwired counterparts. In addition, the observed throughput of wireless communications, because of the effects of multiple access, fading, noise, and interference conditions, is often much less than a radio's maximum transmission rate.
Energy-constrained operation: Most of all the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design optimization criteria may be energy conservation.
Security: Mobile wireless networks are generally more prone to physical security threats than fixed-cable networks. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered.

These characteristics and challenges create a set of essential assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed Internet.

2.3 AODV (AD-HOC ON-DEMAND DISTANCE VECTOR) PROTOCOL

AODV [1] is inherently a distance vector routing protocol that has been optimized for ad-hoc wireless networks. It is an on demand protocol as it finds the routes only when required and is hence also reactive in nature. AODV borrows basic route establishment and maintenance mechanisms from the DSR protocol and hop-to-hop routing vectors from the DSDV protocol. To avoid the problem of routing loops, AODV makes extensive use of sequence numbers in control packets [5].

When a source node intends communicating with a destination node whose route is not known, it broadcasts a RREQ (Route Request) packet. Each RREQ packet contains an ID, source and the destination node IP addresses and sequence numbers together with a hop count and control flags. The ID field uniquely identifies the RREQ packet; the sequence numbers inform regarding the freshness of control packets and the hop-count maintains the number of nodes between the source and the destination. Each recipient of the RREQ packet that has not seen the Source IP and ID pair or doesn't maintain a fresher (larger sequence number) route to the destination rebroadcasts the same packet after incrementing the hop-count. Such

intermediate nodes also create and preserve a REVERSE ROUTE to the source node for a certain interval of time [1][5].

When the RREQ packet reaches the destination node or any node that has a fresher route to the destination a RREP (Route Reply) packet is generated and unicasted back to the source of the RREQ packet. Each RREP packet contains the destination sequence number, the source and the destination IP addresses, route lifetime together with a hop count and control flags. Each intermediate node that receives the RREP packet, increments the hop count, establishes a FORWARD ROUTE to the source of the packet and transmits the packet on the REVERSE ROUTE.

For preserving connectivity information, AODV makes use of periodic HELLO messages to detect link breakages to nodes that it considers as its immediate neighbors. In case a link break is detected for a next hop of an active route a RERR (Route Error) message is sent to its active neighbors that were using that particular route. Optionally, a Route Reply Acknowledgement (RREP-ACK) message may be sent by the originator of the RREQ to acknowledge the receipt of the RREP. RREP-ACK message has no mutable information.

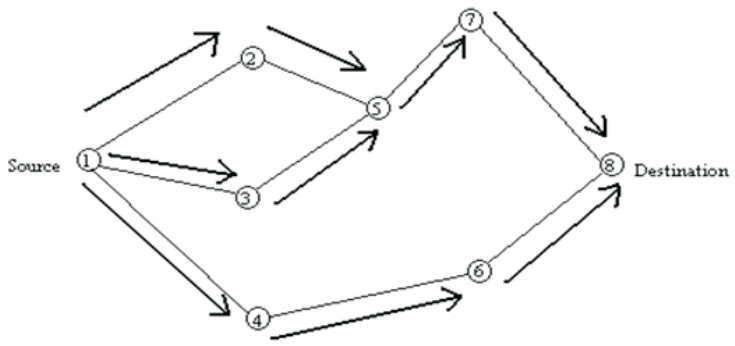
There are two phases of AODV routing protocol: Route Discovery Phase and Route Reply Phase.· Route discovery [4]:

Route Request Stage—the source node floods the network with a route request control packet (RREQ), and each node (with the exception of destination) rebroadcasts the RREQ the first time it hears as shown in fig. 2.1 (a).

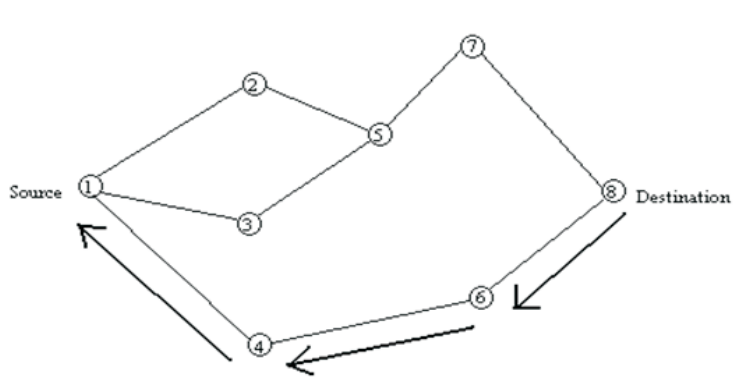
Route Reply Stage—upon receiving a RREQ, the destination sends a route reply packet (RREP), which is propagated to the source in the reverse path of the RREQ as shown in fig. 2.1 (b).

Route maintenance [4]:

If an intermediate node is unable to transmit a data packet to the next hop in the path, it sends a route error control packet (RERR) to the source to inform the broken route.



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

3 LITERETURE REVIEW

3.1SECURITY FLOWS OF AODV ROUTING PROTOCOL

The major vulnerabilities present in the AODV are: (i) Deceptive incrementing of sequence numbers and (ii) Deceptive decrementing of hop-count.

Actually there are seven main requirements to secure AODV protocol properly.

A. Authorized nodes to perform route computation and discovery
B. Minimal exposure of network topology
C. Detection of spoofed routing messages
D. Detection of fabricated routing messages
E. Detection of altered routing messages
F. Avoiding formation of routing loops
G. Prevent redirection of routes from shortest paths

Moreover since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out the following attacks (among many others) against AODV:

1. Impersonate a node S by forging a RREQ with its address as the originator address.
2. When forwarding a RREQ enervated by S to discover a route to D, reduce the hop count field to increase the chances of being in the route path between S and D so it can analyze the communication between them.
3. Impersonate a node D by forging a RREP with its address as a destination address.
4. Impersonate a node by forging a RREP that claims that the node is the destination and, to increase the impact of the attack, claims to be a network leader of the subnet SN with a big sequence number and send it to its neighbors.
5. Electively, not forward certain RREQs and RREPs, not reply to certain RREPs and not forward certain data messages.

3.2 WAYS OF SECURING AODV

It is assumed that there is a key management sub-system that makes it possible for each ad hoc node to obtain public keys from the other nodes of the network. Further, each ad hoc node is capable of securely verifying the association between the identity of a given ad hoc node and the public key of that node. How this is achieved depends on the key management scheme.

3.2.1 SAODV (Secure AODV) Routing Protocol

Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). For the non-mutable information, authentication is performing in an end-to-end manner, but the same kind of techniques cannot be applied to the mutable information. The figures given above show the structure of the AODV messages and indicate what the mutable fields of the messages are.

Secure AODV hash chains[7]

Secure AODV uses hash chains to authenticate the hop count of RREQ and RREP messages in such a way that allows every node that receives the message (either an intermediate node or the final destination) to verify that the hop count has not been decremented by an attacker.

Secure AODV digital signatures[7]

Digital signatures are used to protect the integrity of the non-mutable data in RREQ and RREP messages. That means that they sign everything but the Hop Count of the AODV message and the Hash from the Secure AODV extension. When a RREQ is received by the destination itself, it will reply with a RREP only if it fulfills the AODV's requirements to do so. This RREP will be sent with a RREP Signature Extension. When a node receives a RREP, it first verifies the signature before creating or updating a route to that host. Only if the signature is verified, will it store the route with the signature of the RREP and the lifetime.

SAKM

Simple Ad hoc Key Management (SAKM) provides a key management system that makes it possible for each ad hoc node to obtain public keys from the other nodes of the network. Further, each ad hoc node is capable of securely verifying the association between the identity of a given ad hoc node and the public key of that node. This is achieved by using statistically unique and cryptographically verifiable address.

3.2.2 A-SAODV (Adaptive SAODV) Routing Protocol [5]

To test MANET secure routing in real world scenarios, authors were developed Adaptive SAODV (ASAODV), a prototype implementation of SAODV, based on the AODV-UU implementation by Uppsala University.2 Unlike AODV-UU, A-SAODV is a multithreaded application: cryptographic operations are performed by a dedicated thread to avoid blocking the processing of other messages. Therefore, in A-SAODV, there are two execution threads: one dedicated to cryptographic operations and the other to all other functions (routing message processing, SAODV routing table management, timeout management, SAODV message generation, and data packet forwarding). The two threads communicate via a first input first output (FIFO) queue containing all the messages that must be signed or verified. A-SAODV runs on Linux.

This prototype includes an experimental feature, the adaptive reply decision, which is the reason why it is called A-SAODV (i.e., adaptive SAODV). This feature is meant to optimize SAODV performance with respect to the double signature option. In AODV, allowing intermediate nodes to generate RREPs on behalf of the destination node has a positive impact on performance, because it does not require heavyweight operations by intermediate nodes themselves. The situation is different in SAODV, because generating such a reply requires the intermediate node to generate a cryptographic signature: nodes may spend much time in computing these signatures and become overloaded. Moreover, if intermediate nodes have a long queue of routing messages that must be cryptographically processed, the resulting delay may be longer than if the request reaches the destination node. If we remove the double signature mechanism, we have an uncollaborative protocol, in which only the destination node is allowed to reply to a RREQ message. Therefore, this proposal makes the double signature feature adaptive: intermediate nodes reply to RREQs only if they are not overloaded.

SAODV adds security to AODV but includes cryptographic operations that can have a significant impact on performance. Authors discussed the adaptive reply decision, an experimental feature that added to the implementation to improve SAODV performance. Other possible improvements could be added, for example, delayed verification (which seems to have a positive impact on performance), but further investigation is required. In particular, situations with both “good” and “bad” nodes should be considered in simulation tests to evaluate the behavior of SAODV and of the proposed optimizations under attack (e.g., denial of service attempt).

Successful delivery of RREP messages are important in on-demand routing protocols for ad hoc networks. The loss of RREPs causes serious impairment on the routing performance. This is because the cost of a RREP is very high. If the RREP is lost, a large amount of route discovery effort will be wasted. Furthermore, the source node has to initiate another round of route discovery to establish a route to the destination. The results show that R-AODV improves the performance of AODV in most metrics, as the packet delivery ratio, end to end delay, and energy consumption. Future work is proposed to study practical

design and implementation of the R-AODV.

3.3 REVIEW OF SECURITY PROPOSALS FOR MANETS

There are two approaches of security in MANETs [7][8]: Proactive and Reactive. Both the approaches have their own advantages and are suitable for addressing different issues of MANET's security. For example, most secure routing protocols have proactive approach, while reactive approach is widely used to protect packet forwarding operations. In addition to these, security encompasses three main components: prevention, detection and reaction. In the MANETs, the prevention component is mainly achieved by secure ad hoc routing protocols that prevent the attacker from installing incorrect routing states at other nodes. These protocols are based on earlier ad hoc routing protocols like DSR, AODV, DSDV and employ different cryptographic primitives (e.g. HMAC, digital signature, hash chains) to authenticate the routing messages. Detection observes abnormal behavior of malicious node if any. Once an attacker node is detected, the reaction component makes adjustment in routing and forwarding operations.

Network Layer Security

According to earlier proposals, network layer security has two categories: secure ad hoc routing protocols and secure packet forwarding protocols. Here I would like to discuss only secure ad hoc routing protocols with its possible solutions because there is no much work done in this area. There are several cryptographic primitives for message authentication, the essential component in any security design like HMAC (Message Authentication Codes), Digital Signature, Hash Chains etc.

Secure Ad hoc Routing

This takes the proactive approach and enhances the existing ad hoc routing protocols, such as DSR and AODV, with security extensions. In these protocols, each mobile node proactively signs its routing messages using the cryptographic authentication primitives described above. This way, collaborative nodes can efficiently authenticate the legitimate traffic and differentiate the unauthorized packets from outsider attackers.

Following are the major two types of routing protocols.

Source Routing [8]

The main challenge is to ensure that each intermediate node cannot remove existing nodes from the route or add extra nodes to the route. The basic technique is to attach a per-hop authenticator for the source routing forwarder list so that any altering of the list can be immediately detected. A secure extension of DSR is Ariadne that uses a one-way HMAC key chain for the purpose of message authentication.

Distance Vector Routing [8]

For the DVR protocols such as AODV and DSDV, the main challenge is that each intermediate node has to advertise the routing metric correctly. For example, when hop count is used as the routing metric, each node has to increase the hop count by one exactly. A hop count hash chain is devised so that an intermediate node cannot decrease the hop count in a routing update. Note that a hash chain for this purpose does not need time synchronization, which is different from one-way HMAC key chain for authentication.

4.CONCLUSION AND FUTURE WORK

I have identified that existing system Adhoc on demand distance vector routing protocol is specially designed for mobile adhoc networks with reduced overhead using Expanding Ring Search technique. But energy consumption should also be considered in MANET due to battery constrain of the

nodes. I propose an energy efficient route discovery process for AODV based on ERS.

In the future, I am going to propose a novel security scheme which integrates digital signature and hash chain mechanism to protect the AODV routing protocol that is capable of defending itself against both malicious and unauthenticated nodes with marginal performance difference and also it will consume less energy compared to various existing secure techniques. The proposed security scheme is also planned to simulate on Network Simulator 2 (NS2).

5.REFERENCES

[1] Pirzada, McDonald, *"Secure Routing with the AODV Protocol" (2005) IEEE pp.57-61*

[2] S. Preethi,B.Ramchandran,*"Energy Efficient ROuting Protocols for Mobile Adhoc Networks" IEEE,2011.*

[3] Sandhya Khurana Neelima Gupta and Nagender Aneja, *"Reliable Ad-hoc On-Demand Distance Vector Routing Protocol", (IEEE) Year: 2006, 0-7695-2552-0/06*

[4] Jaa.S. Dalghan, Mohamad M. Gamloush, Raji M. Zeitouny, and Yasser M. Shaer, *"Securing Mobile Adhoc Networks"*

[5] Davide Cerri, Alessandro Ghioni, *"Securing AODV: The A-SAODV Secure Routing Prototype"*, IEEE 2008

[6] Vinay Rishiwal,Ashwani Kush and Shekhar Verma, *" Stable and Energy Efficient* Routing for Mobile Adhoc Networks

[7] Durgesh Wadbude, Vineet Richariya, *"An Efficient Secure AODV Routing Protocol in MANET", IJEIT, 2012*

[8] Stephan Eichler and Christian Roman, *"Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC", Aug 2006.*

[9] The Network Simulator – NS2. (http://www.isi.edu/nsnam/ns/index.html)

[10] The ns Manual, (formerly ns Notes and Documentation) The VINT Project a Collaboration between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC, Kevin Fall, pp. 160

NIRAJ THAKOR
Student, M.E. (CSE) , Parul Institute of Technology, Vadodara, Gujarat Technical University.