Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 4.886|
Vol. 07 Issue 03, March- 2012
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

Security aspects in Ad hoc networks

Vishal Dattana
Research Scholar,
Monad University, Hapur (2011-2013)
Mail: vishaldattana@gmail.com
Bharat Bhushan
Department of Computer Science
Guru Nanak Khalsa College Karnal – Haryana , India

Abstract:

A Mobile Ad Hoc Network (MANET)have some special characteristic features such as unreliable wireless links used for communication between hosts, constantly changing network topologies, limited bandwidth, battery power, low computation power etc. While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are either absent or less severe in wired networks. MANETs are vulnerable to various types of attacks including passive eavesdropping, active interfering, impersonation, and denial-of-service. Intrusion prevention measures such as strong authentication and redundant transmission should be complemented by detection techniques to monitor security status of these networks and identify malicious behavior of any participating node(s). The paper gives an idea of issue and proposed scheme for this.

Introduction:

A Mobile Ad Hoc Network (MANET) [1][2] is a group of mobile nodes that cooperate and forward packets for each other. Such networks extend the limited wireless transmission range of each node by multi-hop packet forwarding, and thus they are ideally suited for scenarios in which predeployed infrastructure support is not available.

The wireless network can be classified into two types: Infrastructured or Infrastructure less. In Infrastructured wireless networks, the mobile node can move while communicating, the base stations are fixed and as the node goes out of the range of a base station, it gets into the range of another base station. In Infrastructureless or Ad Hoc wireless network, the mobile node can move while communicating, there are no fixed base stations and all the nodes in the network act as routers. The mobile nodes in the Ad Hoc network dynamically establish routing among themselves to form their own network 'on the fly'. A Mobile Ad Hoc Network is a collection of wireless mobile nodes forming a temporary/short lived network without any fixed infrastructure where all nodes are free to move about arbitrarily and where all the nodes configure themselves. In this network, each node acts both as a router and as a host & even the topology of network may also change rapidly. Some of the challenges in this network include[14] Unicast/Multicast routing, Dynamic network topology, Network overhead, Scalability, QoS, Stable routing, Secure routing and Power aware routing

Recent work:

A routing protocolis the mechanism by which user traffic is directed and transported through the network from the source node to the destination node. Objectives include maximizing network performance from the application point of view - application requirements- while minimizing the cost of network itself in accordance with its capacity. The application requirements are hop count, delay, throughput, loss rate, stability, jitter, cost; and the network capacity is a function of available resources that reside at each node and number of nodes in the network as well as its density, frequency of end-to-end connection (i.e. number of communication), frequency of topology changes (mobility rate). The four core basic routing functionality for mobile ad hoc networks are:

- *Path generation*: which generates paths according to the assembled and distributed state information of the network and of the application; assembling and distributing network and user traffic state information?

- *Path selection*: which selects appropriate paths based on network and application state information?
- *Data Forwarding*: which forwards user traffic along the select route forwarding user traffic along the selected route?
- *Path Maintenance*: maintaining of the selected route.
- A routing protocol is needed whenever a packet needs to be transmitted to a destination via number of nodes and numerous routing protocols have been proposed for such kind of ad hoc networks. These protocols find a route for packet delivery and deliver the packet to the correct destination. The studies on various aspects of routing protocols have been an active area of research for many years. Many protocols have been suggested keeping applications and type of network in view. Basically, routing protocols can be broadly classified into two types as: Table Driven Protocols or Proactive Protocols and On-Demand Protocols or Reactive Protocols. In Table Driven routing protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes keep on updating these tables to maintain latest view of the network. Some of the existing table driven protocols are DSDV [18, 23], DBF [19], GSR [25], WRP [24] and ZRP [28, 22]. In on-demand routing protocols, routes are created as and when required. When a transmission occurs from source to destination, it invokes the route discovery procedure. The route remains valid till destination is achieved or until the route is no longer needed. Some of the existing on demand routing protocols are: DSR [20, 21], AODV [16, 17] and TORA [26, 27]. The emphasis in this research paper is concentrated on the performance analysis of two prominent on-demand routing Protocols i.e. DSR and AODV.

Due to its characteristics, other desirable features of ad hoc routing protocol include- fast route establishment, multiple routes selection, energy/bandwidth efficiency and fast adaptability to link changes. Almost all routing systems respond in some way to the changes in network and user traffic state. However, routing systems vary widely in the types of *state* changes to which they respond and the speed of their response. Routing states can be divided into three categories -

Static, Quasi Static and Dynamic. Further, each of the three basic routing functions may be implemented in three ways- Centralized, Decentralized and Distributed. The routing protocols can be mainly categorized as: Flat routing, Hierarchical routing and Location aware routing.

Security issues have been raised by A.K verma [4] which shows Wireless mobile ad hoc networks present difficult challenges to routing protocoldesigners. Mobility, constrained bandwidth, and limited power cause frequent topologychanges. The very basic nature of the mode of communication is the main concern because anything that moves over the open air medium is susceptible to be picked up by unauthorizedaccess. For any mission critical or organizationally sensitive information, ad hoc networksadd an element of insecurity. In the existing secure routing protocols most of the security attacksare possible with a compromised node.

A Kush [13] saysan attempt has been made to present an overview of the existing security scenario in the Ad-Hoc network environment. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. These leavesAd-hoc networks wide open for research to meet this demanding application. The existing proposals are typically attack oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats.

Yih-Chun Hu [7] described a rushing attack, a novel and powerful attack against on-demand ad hoc network routing protocols. This attack allows an attacker to mount a denial-of-service attack against all previously proposed secure on-demand ad hocnetwork routing protocols. We have also presented RAP (Rushing Attack Prevention), a new protocol that thwarts the rushing attack.

SrinathPerur[15]presented a preemptive route repair strategy for AODV called Router Handoff. He found that in most cases tested it reduces routing overhead and improves throughput. He also believes that the concept of handoff could be used in contexts other than link failure. For instance, a node that is low on power, or a node that knows it is going to switch off could handoff without affecting the rest of the ad hoc network.

Security issue:

As previously stated, many applications have recently become dependent on *ad hoc* wireless networks, and security is an extremely serious issue in any network.[4][5] The dynamic nature of *ad hoc* wireless networks makes it extremely challenging to ensure secure transmission in these networks , which rely on the collaboration of all their nodes for their creation and efficient operation. While maintaining suitable routing information in a distributed way is a challenging issue in such networks, it is even more challenging to secure the protocols used for routing. At the network level, an *ad hoc* system fundamentally requires the routing protocols to be secured, as they enable a communication path to be established.

There are many different types of existing routing protocols that have been extensively researched with a view to finding solutions to such security vulnerabilities, but none has so far satisfied all of the requirements of a secure routing protocol, which are:

- Confidentiality: [6]ensures that only authorised users can access or reveal transmitted messages;
- Integrity: [7]ensures that unauthorised persons cannot modify, alter or retransmit data to another destination;
- Authentication: [8]ensures that both end-peers are who they claim to be;
- Non-repudiation:[9] ensures that the sender/receiver cannot deny sending/receiving;
- Guarantee of correct route discovery: ensures that the protocol is able to find the route and the correctness of the selected route;
- Stability against attacks: ensures that the protocol is able to revert to its normal operation after any attack;
- Availability: [10]ensures that resources and entities are available when needed by the intended parties.

The problems of existing approaches can be summarised thus:

- They fail to satisfy all security requirements;
- Each secure routing protocol is designed to detect or prevent specific attacks;
- They are extensions of existing routing protocols without resolving their problems;
- They fail to deal with hostile environments;
- They have insecure node-to-node paths.

The objective of the work is to find solutions to the above problems by:

- Designing new adaptive approaches to the routing of *ad hoc* wireless networks based on exist protocols;
- Analysing the existing protocols and resolving their problems;
- Designing a new secure routing protocol based on secure node-to-node paths.
- Ensuring that the secure routing protocol satisfies all requirements via applied security mechanisms;

Using the history of nodes to access a hostile environment; and satisfying all requirements to protect against or prevent almost all attacks.

Proposed scheme:

Mobile ad hoc networks are being widely deployed currently since they provide some features, which are difficult or impossible to be achieved by conventional networks. The application area ranges from the battlefield (sensor nodes in hostile territory) to general transportation that provide useful infrastructure during disaster recovery

A brief review of AODV is presented here as the proposed scheme has been incorporated on AODV.

In the reactive protocol AODV, [11] [12] a node discovers or maintains route to a destination if andonly if it is the initiator of the route to that destination or is an intermediate node on an activeroute to that destination. Otherwise, it does not maintain routing information to that destination. AODV maintains loop-free routes, even when the local connectivity for a node on the route changes. This is achieved by maintaining a counter for eachnode, called a sequence number. This sequence number of a node is incremented every time the local connectivity of the node changes. In AODV, the route discovery is initiated by the sourceby generating and broadcasting a route request packet RREQ. The RREQ packet contains sequencenumbers for source as well as destination nodes, called source-sequence-num and destination-sequence-num, respectively. When a node receives a RREQ packet, if the node is itself the destination or it has a valid route to that destination, it determines the freshness of its route table entry (provided such an entry exists) for that destination by comparing the destination-sequence-num in the RREQ with that of its route table entry. The node then either responds with a route reply RREP (if it itself is the destination or has a fresh route to that destination) or rebroadcasts the RREQ to its neighbors. The node makes an entry for this route request in the route table and stores the address of the node from which it received this request as the next hop in the route to the source of this request packet. Similarly when a node receives a response RREP for the request it stores the address of the node from which it received the response RREP as the next hop in the route to that destination. As the RREP travels back to the source, the intermediate nodes forwarding the RREP, update their routing tables with a route to the destination. The RREP has a field for destination-sequence-num.

Route Construction (REQ) Phase

This scheme can be incorporated with reactive routing protocols that build routes on demand via a query and reply procedure. The scheme does not require any modification to the AODV's RREQ (route request) propagation process. In BBR (Backbone based Routing) when a source needs to initiate a data session to a destination but does not have any route information, it searches a route by flooding a ROUTE REQUEST (REQ) packet. Each REQ packet has a unique identifier so that nodes can detect and drop duplicate packets. An Intermediate node with an

active route, upon receiving a no duplicate REQ, records the previous hop and the source node information in its route table. It then broadcasts the packet or sends back a ROUTE REPLY (REP) packet to the source if it has an active routeto the destination. The destination node sends a REP via the selected route when it receives the first REQ or subsequent REQs that traversed a better active route. Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, an ERR message is used to notify that the loss of link has occurred to its one hop neighbor. Here ERR message indicates those destinations which are no longer reachable by way of the broken link. Taking advantage of the broadcast nature of wireless communications, a node promiscuously overhears packets that are transmitted by their neighboring nodes. When a node that is not part of the route overhears a REP packet not directed to itself transmit by a neighbor (on the primary route), it records that neighbor as the next hop to the destination in its alternate route table. From these packets, a node obtains alternate path information and makes entries of these backbone nodes (BN) in its route table. If route breaks occurs it just starts route construction phase from that node. The protocol updates list of BNs periodically in the route table.

Route Error and Maintenance (REP) Phase

Data packets are delivered through the primary route unless there is a route disconnection. When a node detects a link break (for example, receives a link layer feedback signal from the MAC protocol, node1 does not receive passive acknowledgments, node2 does not receive hello packets for a certain period of time, etc.), it performs a one hop data broadcast to its immediate neighbors. The node specifies in the data header that the link is disconnected and thus the packet is candidate for alternate routing. Upon receiving this packet, previous one hop neighbor starts route maintenance phase and constructs an alternate route through backbone nodes by checking their stability.Nodes those have an entry for the destination in their alternate route table; transmit the packet to their next hop node. Data packets therefore can be delivered through one or more alternate routes and are not dropped when route breaks occur. To prevent packets from tracing a loop, these mesh nodes forward the data packet only if the packet is not received from their next hop to the destination and is not a duplicate. When a node of the primary route receives the data

packet from alternate routes, it operates normally and forwards the packet to its next hop when the packet is not a duplicate. All this route maintenance occurs under *local repair* scheme.

Route Erasure (RE) phase

When a discovered route is no longer desired, a route erasure broadcast will be initiated by Source, so that all nodes will update their routing table entries. A full broadcast is needed because some nodes may have changed during route reconstruction. RE can only be invoked by SRC (source).

Conclusion:

A new protocol has been proposed which will be incorporated on AODV. As the topic of the research is to provide stability in MANET, so in the proposed algorithm these issues are taken into account. It is basically the enhancement of the existing AODV algorithm as it provides better stability in normal working. The proposed scheme will be simulated extensively using NS2as network simulator and various metrics used will be; **Packet Delivery Ratio: Throughput: Average end to end delay and Control packet overhead.**

References:

[1]National Science Foundation, "Research priorities in Wireless and mobile networking", available at www.cise.nsf.gov.

[2] C. E. Perkins, "Ad Hoc Networking," Addison-Wesley Longman, 2000.

[3]B. Anand and S. Papavassiliou, "A mobility-based clustering approach to support mobility management and multicast routing in mobile ad-hoc wireless networks," International J. of Network Management, vol. 11, pages 387-395, 2001.

[4] A. K. Verma, Mayank Dave and R C Joshi, "Secure Routing in Mobile Networks: A Review," *International J. of Systemics, Cybernetics and Informatics (IJSCI), ISSN 0973-4864*

[5] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," *In Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, 2002.

[6] A. K. Verma, Mayank Dave and R C Joshi, "Secure Data Sharing inMobileAdhoc Networks," *J. International Review on Computers andSoftware (IRECOS), ISSN 1828-6003* (Peer reviewed and accepted).

[7] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," *In Proc. ACM workshop on Wireless security*, 2003.

[8] M. Reiter and S. Stybblebine, "Authentication Metric Analysis and Design," *ACM Transactions on Information and System Security*, 1999.

[9] Daniel B. Faria and David R. Cheriton, "DoS and Authentication in Wireless Public Access Networks," *In Proc. of the 1st ACM Workshop on Wireless Security"* (WiSe'02), September 2002.

[10] A.Kush, Sunil Tanjea, "**End to End Delay Analysis of Prominent On-demand Routing Protocols"** IJCST, International Journal of Computer Science and Technology, Vol 2 Issue 1 March 2011, I S SN : 2 2 2 9 - 4 3 3 3 (P r i n t) | I S S N : 0 9 7 6 - 8 4 9 1 (On l i n e) pp 42-46

[11] C. E. Perkins, E. M. Belding-Royer, and S. Das.Ad hoc On-Demand Distance Vector (AODV) Routing.*RFC 3561*, July 2003.

[12] C. E. Perkins and E. M. Royer. The Ad hoc On-Demand Distance Vector Protocol. In C. E. Perkins, editor, *Ad hoc Networking*, pages 173.219. Addison-Wesley, 2000.

[13] A.Kush "Security Aspects in AD hoc Routing", Computer Society of India ommunications, Vol no 32Issue 11, March 09 pp 29-33.

[14] Sunil Taneja, A.Kush "PERFORMANCE EVALUATION OF DSR AND AODV OVER UDP AND TCP CONNECTIONS" International Journal of Computing and Business Research (IJCBR) Volume 1, N. 1 December - 2010

[15] SrinathPerur, Abhilash P. and Sridhar Iyer "Router Handoff: A Preemptive Route Repair Strategy for AODV" K.R. School of Information Technology, IIT Bombay.

[16] A. Kush, R.Chauhan, C.Hwang and P.Gupta, "Stable and Energy Efficient Routing for Mobile Adhoc Networks", Proceedings of the Fifth International Conference on Information Technology: New Generations, ISBN:978-0-76953099-4 available at ACM Digital Portal, pp. 1028-1033, 2008.

[17] C. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing - Internet Draft", RFC 3561, IETF Network Working Group, July 2003.

[18] C. E. Perkins and E. M. Royer, "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2 nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA, pp. 90-100, 1999.

[19] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers", Proceedings of ACM SIGCOMM 94, pp. 34–244, 1994.

[20] D. Bertsekas and R. Gallager, "Data Networks" Prentice Hall Publ., New Jersey, 2002.

[21] D. B. Johnson, D. A. Maltz, Y.C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Draft, http://www.ietf.org/internetdrafts/draft-ietf-manet-dsr-09.txt, April 2003.

[22] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Networks", Mobile Computing, T. Imielinski and H. Korth, Eds., Kulwer Publ., pp. 152-81, 1996.

[23] Farhat Anwar, Md. Saiful Azad, Md. ArafaturRahman, Mohammad MosheeUddin, "Performance Analysis of Ad hoc Routing Protocols in Mobile WiMAX Environment", IAENG International Journal of Computer Science, 35:3, IJCS_35_3_13.

[24] P. Chenna Reddy, Dr. P. Chandrasekhar Reddy, "Performance Analysis of Adhoc Network Routing Protocols", Academic Open Internet Journal, Volume 17, 2006. International Journal of Computing and Business Research (IJCBR) Volume 1, N. 1 December - 2010

[25] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. Journal, Special Issue on Routing in Mobile Communication Networks, pp. 183-97, 1996.

[26] Tsu-Wei Chen and M. Gerla, "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks", Proceedings of International Computing Conference IEEE ICC 1998.

[27] V. Park and S. Corson, Temporally Ordered Routing Algorithm (TORA) Version 1, Functional specification IETF Internet draft, http://www.ietf.org/internet-drafts/draft-ietf-manet-tora-spec-01.txt, 1998.

[28] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), Kobe, Japan, pp. 1405-1413, 1997.