Journal of Advances in Science and Technology

Vol. IV, No. VII, November-2012, ISSN 2230-9659

A SECURE MANETS TRACKING PROTOCOLS WITH VERSATILITY OPPOSITE BYZANTINE BEHAVIORS OF MALICIOUS OR SELFISH NODES

www.ignited.in

Journal of Advances in Science and Technology
Vol. IV, No. VII, November-2012, ISSN 2230-9659

A Secure Manets Tracking Protocols With Versatility opposite Byzantine Behaviors of Malicious or Selfish Nodes

Om Prakash Gera

Research Scholar, Sri Venkateshwara University, Amroha (U.P.)

Abstract – Secure routing in mobile ad hoc networks (MANETs) has emerged as a important MANET research area. MANETs, by virtue of the fact that they are wireless networks, are more vulnerable to intrusion by malicious agents than wired networks. In wired networks, appropriate physical security measures, such as restriction of physical access to network infrastructures, can be used to attenuate the risk of intrusions. Physical security measures are less effective however in limiting access to wireless network media. Consequently, MANETs are much more susceptible to infiltration by malicious agents. Authentication mechanisms can help to prevent unauthorized access to MANETs. However, considering the high likelihood that nodes with proper authentication credentials can be taken over by malicious entities, there are needs for security protocols which allow MANET nodes to operate in potential adversarial environments.

In this paper, we present a secure on-demand MANET routing protocol, we named Robust Source Routing (RSR). In addition to providing data origin authentication services and integrity checks, RSR is able to mitigate against intelligent malicious agents which selectively drop or modify packets they agreed to forward. Simulation studies confirm that RSR is capable of maintaining high delivery ratio even when a majority of the MANET nodes are malicious.

In recent years, many protocols have been proposed to secure the routing process in mobile ad-hoc networks (MANETs). However, there are still many security issues that have not been fully resolved by these algorithms. Selfishness of independent nodes locally degrades network routing efficiency. Also malicious nodes can easily corrupt the performance of the MANET by showing their Byzantine behaviors and so what is called a wormhole attack. One of the solutions to defeat the collaborating of malicious nodes is multipath routing algorithms that can withstand the failure of the primary path and provide alternate paths between the source and destination when such attacks happen.

---------------------------♦-----------------------------

INTRODUCTION

Research have shown that misbehaving nodes in a MANET can adversely affect the availability of services in the network. Nodes misbehave either because they are broken, selfish or malicious. Broken nodes are non-functional. A node can agree to forward traffic on behalf of other nodes but becomes nonfunctional prior to it fulfilling this agreement. Selfish nodes can agree to forward packets but silently drop the packets in attempt to conserve energy and bandwidth. Malicious nodes may seek to disrupt a network and hide their malicious behaviour by selectively dropping packets they agreed to forward. They may also attempt to create denial of service exploits by injecting large number of packets into the network. Most of the MANET secure routing schemes in research literature, for example, do not militate against these misbehaviors.

In this paper, we present a robust secure on-demand multipath source routing protocol which effectively mitigates against selective packet dropping and other adversarial activities. To the best of our knowledge, our work is the first documented effort to utilize the concept of forerunner packets to encourage cooperation in ad hoc networks.

Mobile Ad-hoc Networks (MANETs) are characterized by mobile hosts connected by wireless links communicating with each other without any infrastructure such as access point or base station. MANETs have many applications in a wide area of situations. MANET applications include military and emergency instances to establish an integrated network in an infrastructure-less location. Also MANETs are used for sensor networks, civilian applications, and ubiquitous computing. We could imagine most of the applications of infrastructure-based networks for MANETs with mobility feature.

Each ad-hoc node can only communicate with its neighbor nodes within its radio range. Each node to send a message to the node out of its radio range has to ask its neighbor nodes' help. So a multi-hop path between source and destination must be discovered. As the hosts of MANET move randomly, the topology of the MANET changes.

MANET is usually established for impromptu decisions to achieve the specific goal. As mentioned we could conclude the main characteristics of MANET such as: wireless autonomous nodes, ad-hoc-based network, multi-hop routing protocols, mobility, and infrastructure-less. Many routing protocols have been suggested to find multihop routes between some nodes. But selfish and malicious nodes can disrupt found paths easily. Routing protocol designers try to secure their schemes by using cryptography methods like confidentiality, integrity, authentication and non-repudiation. But these methods are not enough to establish connection. One of the main security services mentioned in network security is *availability* that is needed to assure establishing connection. Providing availability service is a challenging issue like DoS attack resiliency and cannot be achieved by using cryptography methods lonely.

Wireless ad-hoc network is a computer network that uses wireless communication links. In wireless adhoc networks each node is willing to forward data for other nodes. This is in contrast to wired network technologies in which the task of forwarding the data is performed using some designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls.

In addition, it is in contrast to managed wireless networks in which a special node known as an access point manages communication among other nodes is used. Mobile ad hoc networks (MANETs), Wireless mesh networks, and wireless sensor networks are the three types of wireless ad-hoc networks. The Ad hoc networks are appropriate for emergency situations like natural disasters or military conflicts due to their minimal configuration and quick deployment. They are appropriate for a variety of applications where central nodes cannot be relied on due to the decentralized nature of most wireless ad hoc networks that in comparison to wireless managed networks improve the scalability of wireless ad-hoc networks.

Routing protocols for ad hoc networks generally can be divided in to two main categories: *periodic* protocols and *on-demand* protocols. In a periodic (or proactive) routing protocol, nodes periodically exchange routing information with other nodes in an attempt to have each node always know a current route to all destinations . In an on-demand (or reactive) protocol, on the other hand, nodes exchange routing information only when needed, with a node attempting to discover a route to some destination only when it has a packet to send to that destination.The proposed protocol is an on-demand (reactive) protocol that provides resilience against Byzantine attacks.

A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected wirelessly. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network. Therefore, this kind of wireless network can be viewed as mobile ad hoc network.

FUNDAMENTAL CONCEPTS

On-demand Distance Vector Routing : Routing protocols in wireless networks are for the most part based on either separation vector or source steering and not connect state tracking equations. Tracking ordered systems in provincial networks need intermittent show of steering informative data by every router such as Destination Sequenced Distance Vector (DSDV) as a proactive (occasional) tracking methodology. In separation vector steering, each router shows to every last bit of its neighboring routers the prospected separation to all other non-neighboring junctions.

An additional celebrated around the world notion of steering is source tracking, a system where the source of the bundle verifies the finish succession of the junctions of the built track. Every transitional junction connects its deliver to the header of the bundle such as what happened to Dynamic Source Routing (DSR). In connection-state tracking, every router shows to every last bit of its neighboring routers its perspective of the status of each of its adjoining connections; the neighboring junctions then register the most brief separation to every junction based upon the complete topology of the system such as Optimized Link State Routing (OLSR) . Some protocols such as DSDV, called as proactive, are suitable for system dominions where there are no junction power utilization imperatives. In MANETs where junctions have control imperatives and the system has a considerably increasingly alterable nature, reactive or ondemand tracking protocols are ordinarily utilized. Tracking table overhaul system of on-interest tracking order are unique in relation to the past proactive methodologies. Reactive alternately on-interest steering protocols make and stand by ways from one source to its goal on an as required support.

Contrasted with the proactive partners of the on-interest protocols, the tracking disclosure overhead is normally easier. On-interest track disclosure decreased the expense of track upkeep towards occasional track finding, for the reason that unused tracks are not upgraded. On-interest track finding is suitable when the system activity is inadequate and identified with a known subset of junctions. Anyway information activity endures from the postponement of track disclosure and track upkeep method. Likewise the aforementioned tracking ordered systems, conversely with source tracking, use a more modest header, for the reason that their parcels doesn't pass on the location record of passing routers with the exception of the address of source and goal.

Flooding methodology encourages reactive protocols to find tracks. The activity source surges an analysis bundle called Track Request Packet (RREQ) into the system to discover a track to the longing end. Any time an old track breaks on account of a connection breakage, flooding is moreover had an association with administer another track in place of past track. To have adequate exhibition of reactive protocols flooding technique ought to be regulated, on the grounds that it depletes the by and large measures of system assets like transfer speed and junctions' power.

All of above protocols are single way protocols, for the reason that they find one singular most brief way in the particular topology of the system. Depending on if there are egotistical junctions that don't collaborate for fitting execution of information sending, or pernicious junctions that intrigue to make wormholes, engaged information sending ways may be broken. So track finding process must be performed again. Accordingly it requires flooding RREQs in the system again. In ad-hoc networks with dynamic topology, visit track support demands cause the heightened inertness of new track revelation stage and influence the exhibition proficiency conflictingly.

Multipath Routing : Multipath on-demand routing protocols try to alleviate single path reactive routing protocols flaws by discovering multiple routes in a single route discovery procedure. Source nodes and intermediate nodes could find multipaths sent by destination nodes. Route maintenance stage is needed only when all previous paths fail. So route maintenance latency and routing overheads decrease. By storing more available path to destination, higher performance efficiency could be achieved. Multipath routing in wired networks has been suggested to decrease data re-forwarding, control congestion, and deal with QoS issues. Other coercing advantages of applying multipath routing in MANETs are lower latency, higher fault tolerance, lower energy consumption, and higher robustness. Some on-demand multipath routing protocols have been suggested for ad hoc networks, including Shortest Multipath Routing Using Labeled Distances, Ad hoc On-demand Multipath Distance Vector (AOMDV), Multipath Dynamic Source Routing (Multipath DSR), Cooperative Packet Caching and Shortest Multipath (CHAMP), Temporally Ordered Routing Algorithm (TORA), Split Multipath Routing (SMR), and Routing On-demand Acyclic Multipath (ROAM). SMR and MDSR are on the basis of dynamic source routing whereas AOMDV, ROAM, CHAMP and TORA are destination-sequenced distance vector routing based.

Mentioned protocols establish multiple paths upon request, the data traffic could be distributed into multiple routes. But usually a single route is mainly employed and the other routes are applied only when the main route fails.

OVERVIEW

Network Model : Our suggested ordered system is actualized in the network layer. It is gathered that neighbor revelation stage has been completed by a suitable layer-2 or layer-3 methods. We additionally posit that an affirmation (ACK) gathering technique will execute in the transport layer or network layer that might show revise gathering of source parcels. Any time the source does not appropriate any ACK, it attempts an alternate one track until it can secure a sheltered way. Our posited network topology is a random graph model network, that ad-hoc nodes is erratically set in their positions. Moreover it is posited the junctions aspects are the same.

Attack Scenario Model : Passive and active attacks on availability of safe connections are considered in this paper. Other threats against security services like confidentiality, integrity or non-repudiation by eavesdropping or forging packets have not been included, because some of them could be provided by using cryptographic methods.

Two kinds of selfish nodes including Type-I and Type-II could be available among the nodes. Behavior of a selfish/malicious node is independent from its neighbor nodes' behavior.

Cooperation enforcement schemes need supervising by trusted third party. Third party is like a central bank that gives reputation to its branches. Without any third party, malicious nodes could cheat in reputations. They could generate fake currencies or shows the value of other nodes' reputation lower or higher. So we are not interested in cooperative schemes.

Solution Strategy: Our goal is to establish a connection between the source and the destination.

To counter the effects of wormhole attacks and selfishness, LMAR algorithm creates at least one alternative working path that is established by active cooperators from source to destination. LMAR has been designed such that it could explore all available paths from source to destination in the graph of network topology to get a working route. Theoretically if the induced sub-graph of the network topology is connected by removing selfish and malicious nodes, LMAR can discover a locally efficient path from source to destination.

RELATED WORK

An instrument of distinguishing junction rowdiness regarding narrow-mindedness was put forth by Tarag Fahad and Robert Askwith. The working of their algorithm has been delineated with two situations. Their algorithm PCMA identified self centered junctions which perform full/partial bundles assault in an auspicious way.

A credit-based secure incentive protocol (SIP) that recreates coordination in bundle sending for foundation less MANETs was suggested by Yanchao Zhang. SIP was warily planned to be a secure yet lightweight charging and compensation protocol and to be equipped to withstand an extensive variety of cheating activities. In expansion, SIP utilizes a space-powerful Bloom channel that gave flat conveyance overhead.

The tracking rowdiness in MANETs was concentrated on by Kejun Liu. The 2ACK plan that serves as an include-on strategy for tracking plans to distinguish tracking rowdiness and to alleviate their inimical impact was introduced. So as to send two-bounce affirmation bundles in the inverse bearing of the tracking way, the 2ACK plan was utilized.

A proof-of-concept implementation of a secure routing protocol based on AODV over IPv6, further reinforced by a routing protocol-independent Intrusion Detection and Response system for ad-hoc networks was presented by Anand Patwardhan. The mechanisms for non-repudiation, authentication using Statistically Unique and Cryptographically Verifiable (SUCV) identifiers, without relying on the availability of a Certificate Authority (CA), or a Key Distribution Center (KDC) were included in the security features of the routing protocol . They have also discussed several scenarios where the secure routing and intrusion detection mechanisms isolate and deny network resources to nodes deemed malicious.

Li Zhao and José G. Delgado-Frias have proposed and valuated a Multipath Routing Single path transmission (MARS) scheme to detect misbehavior on data and mitigate adverse effects. To provide more comprehensive protection against misbehavior from individual or cooperating misbehaving nodes, the proposed MARS scheme combined multipath routing, single path data transmission, and end-to-end feedback mechanism together .

Strike opposite tracking in ad hoc networks were introduced by YihChun H. Also, the outline of Ariadne, another secure on-interest ad hoc network tracking protocol was put forth and its exhibition was assessed. Ariadne forestalls ambushers or traded off junctions from tampering with uncompromised tracks comprising of uncompromised junctions. Also, it forestalls an impressive number of sorts of Disavowal-of-Service assaults.

Two systems that enhance throughput in an ad hoc network in the presence of junctions that consent to send parcels yet cannot do so are displayed by Sergio Marti.

They have recommended ordering junctions based upon their progressively measured conduct to alleviate this situation. Keeping in mind the end goal to recognize the getting rowdy junctions they utilized a watchdog. So as to help the steering protocols to evade the aforementioned junctions, a way rater was utilized.

The SMT and SSP protocols for secure information

correspondence in ad hoc networks were put forth and investigated by Panagiotis Papadimitratos and Zygmunt J. Haas. Owing to the way that the two protocols furnish lightweight end-to-end security aids and work without learning of the trustworthiness of single person network junctions, they are connected widely .

An on-interest steering protocol for ad hoc remote networks that furnishes flexibility to byzantine washouts created by single or conspiring junctions was put forth by Baruch Awerbuchl. After log n issues have happened (where n is the length of the way), a vindictive connection is istinguished by their versatile examining strategy. At that point, the weights of the aforementioned connections are multiplicatively expanded and an on-interest track revelation protocol that discovers a slightest weight way to the end is used, consequently the aforementioned connections are evaded.

The idea of a tunneling strike, in which working together pernicious junctions can typify wires between them to subvert tracking measurements, was presented by Kimaya Sanzgiri, et al. A result for secured tracking in the administered-open earth was furnished by their protocol, ARAN. ARAN utilized decided beforehand cryptographic testaments that certifications end-to-end validation to give verification and nonrepudiation utilities.

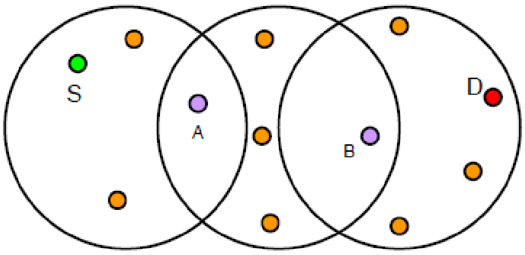
The configuration and assessment of SEAD, a secure ad hoc network tracking protocol utilizing separation vector tracking was introduced by Yih-Chun Hu, et. al. They utilized powerful oneway hash roles and did not utilize deviated cryptographic operations in the protocol to back utilization of junctions with confined CPU preparing capacity and to monitor opposite Denial-of-Service (DoS) assaults in which an assaulter endeavors to create different junctions to deplete overabundance network transfer speed or handling time .

Gergely Acs have contended that imperfections in ad hoc tracking protocols could be exceptionally inconspicuous, and they bolstered a more efficient path of examination. They have suggested a scientific structure in which security might be absolutely outlined and tracking protocols for portable ad hoc networks could be ended up being secure in a meticulous way.

Their system was tailored for on-interest source tracking protocols, yet the general standards are appropriate to different sorts of protocols as well. Their methodology was based on the re-enactment standard, which has as of recently been utilized broadly for the examination of nexus station protocols, yet, to the best of our information, it has not been connected in the setting of ad hoc tracking thus far. They have additionally suggested an on-interest source tracking protocol, called endairA, and showed the utilization of our skeleton by demonstrating that it is secure in our model.

MANET ROUTING SECURITY

In an ad hoc network, all the nodes may not be within the transmission range of each other; hence, nodes are often required to forward network traffic on behalf of other nodes. Consider for example the scenario in Fig. If node S sends data to node D, which is three hops away, the data traffic will reach its destination only of A and B forward it. The process of forwarding network traffic from source to destination is termed routing



.

Figure : Multihop scenario

There are two general categories of MANET routing protocols: topology-based and position-based routing rotocols. The list of some desirable qualitative properties of MANET routing protocols as adopted from an Internet Engineering Task Force (IETF) MANET Working Group memo is as following:

- Loop-free: It is desirable that routing protocols prevent packets from circling around in a network for arbitrary time periods.

- Demand-based operation: In order to utilize network energy and bandwidth more efficiently, it is desirable that MANET routing algorithms adapt to the network traffic pattern on a demand or need basis rather than maintaining routing between all nodes at all time.

- Proactive operation: This is the IP-side of demand-based operation. In cases where the additional latency, which demand-based operations incur, may be unacceptable, if there are adequate bandwidth and energy resources, proactive operations may be desirable in these situations.

- “Sleep" period operation: It may be necessary, for reasons such as the need for energy conservation, for nodes to stop transmitting or receiving signals for arbitrary time periods. Routing protocols should be able to accommodate sleep periods without adverse consequences.

- Security: It is desirable that routing protocols provide security mechanisms to prohibit disruption or modification of the protocol operations.

CONCLUSION

In this paper we presented Robust Source Routing (RSR). RSR is a secure MANET on-demand routing protocol which is capable of delivering packets to their respective destinations even in the presence of large proportions of active malicious or selfish agents which selectively drop packets they are required to forward. RSR introduced the concept of forerunner (FR) packets which inform nodes along a path that they should expect specified data flow within a given time frame. The path elements can therefore be on the look out for the given data flow, and in the event that they do not receive the traffic flow, they can transmit info to the source informing it that the data flow they expected did not arrive. In so doing, links with active malicious agents can be identified, and the malicious agents be eventually isolated.

In this paper, we introduced an efficient local-multipath adaptive routing (LMAR) protocol, a routing algorithm to provide availability security service properly. The objective of LMAR design is to provide a mechanism by which network nodes can find alternative paths using a distributed mechanism. This is done using an exhaustive search algorithm.

Therefore LMAR can bypass the selfishness of independent nodes that disrupt the data path. In addition LMAR could defeat the wormhole attach by finding alternate routes that bypass the wormholes.

In mobile adhoc networks, the Byzantine behavior of authenticated nodes results in route disruption actions. To mitigate these vulnerabilities of routing protocols in wireless adhoc networks, we propose a new Byzantine-Resilient Secure Routing Protocol (BRSR) that provides resilience against Byzantine attacks. Since existing routing protocols provide solutions separately for insider attacks, outsider attacks and selective forwarding attacks, our proposed protocol provides total protection against all these attacks. Through simulation results, we have demonstrated that BRSR effectively mitigates the identified attacks with stronger resistance against node capture by providing better delivery ratio. As a future work, we will try to reduce the overhead and delay of the proposed protocol by maintaining much more resistance against the identified attacks.

This paper presents a number of routing protocols for MANET, which are broadly categorized as proactive and reactive. Proactive routing protocols tend to provide lower latency than that of the on-demand protocols, because they try to maintain routes to all the nodes in the network all the time.

But the drawback for such protocols is the excessive routing overhead transmitted, which is periodic in nature without much consideration for the network mobility or load. On the other hand, though reactive protocols discover routes only when they are needed, they may still generate a huge amount of traffic when the network changes frequently. Depending on the amount of network traffic and number of flows, the routing protocols could be chosen. When there is congestion in the network due to heavy traffic, in general case, a reactive protocol is preferable. Sometimes the size of the network might be a major considerable point. For example, AODV, DSR, OLSR are some of the protocols suitable for relatively smaller networks, while the routing protocols like TORA, LANMAR, ZRP are suitable for larger networks. Network mobility is another factor that can degrade the performance of certain protocols. When the network is relatively static, proactive routing protocols can be used, as storing the topology information in such case is more efficient. On the other hand, as the mobility of nodes in the network increases, reactive protocols perform better. Overall, the answer to the debating point might be that the mobility and traffic pattern of the network must play the key role for choosing an appropriate routing strategy for a particular network. It is quite natural that one particular solution cannot be applied for all sorts of situations and, even if applied, might not be optimal in all cases. Often it is more appropriate to apply a hybrid protocol rather than a strictly proactive or reactive protocol as hybrid protocols often possess the advantages of both types of protocols.

REFERENCES

- J. Binkley and W. Trost. Authenticated ad hoc routing at the link layer for mobile systems. *Wireless Networks*, 7(2):139–145, 2001.

- Boukerche, K. El-Khatib, L. Xu, and L. Korba. An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks. *Computer Communications*, 28(10):1193–1203, 2005.

- L. Buttyan and J.-P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *ACM/Kluwer Mobile Networks and Applications*, 8(5):579–592, 2003.

- K. Chen, K. Nahrstedt, and N. Vaidya. The utility of explicit rate-based

- flow control in mobile ad hoc networks. In *Proceedings of IEEE Wireless Communications and Networking Conference WCNC 2004*, pages 1921–

- 1926 Vol.3, 2004.

- R. Davis. *IPSec: Securing VPNs*. Osborne/McGraw-Hill, New York, 2001.

- T. Clausen and P. Jacquet, RFC 3626: Optimized link state routing protocol (OLSR), October 2003.

- Balasubramanian and J.J. Garcia-Luna-Aceves, Shortest Multipath Routing Using Labeled Distances, Proc. Of 1st IEEE MASS, October 2004.

- M. K. Marina and S. R. Das, on-demand multipath distance vector routing in ad hoc networks, Proc. IEEE ICNP, 2001.

- Nasipuri, R. Castaneda, and S. R. Das, Performance of Multipath Routing for On-Demand Protocols in Mobile Ad Hoc Networks, ACM/Kluwer Mobile Networks and Applications (MONET), 2001.

- Valera, W. Seah, and S. V. Rao, Cooperative packet caching and shortest multipath routing in mobile ad hoc networks, Proc. IEEE INFOCOM, 2003.

- Ovais Ahmad Khan, "A Survey of Secure Routing Techniques for MANET", Course Survey Report, Fall 2003.

- Tarag Fahad & Robert Askwith, "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks”,

- Yanchao Zhang, Wenjing Louy, Wei Liu and Yuguang Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks", in proc. of Journal on Wireless Networks, vol. 13, no. 5, pp: 569- 582, October 2007.

- Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing, vol. 6, no. 5, pp: 536-550, May 2007.

- Anand Patwardhan, Jim Parker and Anupam Joshi, "Secure Routing and Intrusion Detection in Ad Hoc Networks", in proc. of 3rd International Conference on Prevasive Computing and Communications, March 8, 2005.

- M.S. Corson, J.P. Maker, and J.H. Cernicione, Internetbased Mobile Ad Hoc Networking, IEEE Internet Computing, July-August 1999, pp. 63-70.

- Mohammad Ilyas (Ed.), The Handbook of Ad Hoc Wireless Networks CRC Press LLC, Florida, 2003.

- Tarun Dalal, Gopal Singh, An Analysis of ASRP Secure Routing Protocol for MANET, IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 2, Apr. 2012, pp. 132-137.

- Panagiotis Papadimitratos et al., Secure Routing for Mobile Ad hoc Networks, Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, Jan.2002.