Volume 2, No. 1, Jan-Feb 2011

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Mobile Ad Hoc Networks: Evaluation Of Security in Routing Algorithms

Prasuna V G*
Assistant Prof
MCA Department,.,BII
Hyderabad, AndhraPradesh, INDIA
prasuna.panyam@rediffmail.com

Dr. S. Madhusudhana Verma
HOD,
Department of OR & SQC, Rayalaseema University,
Kurnool, AndhraPradesh, INDIA
seeverma@rediffmail.com

Abstract: The outcomes of the Ad Hoc networks expertise advocate substantive wireless correspondence of devices that can transmit or transverse communication amid two nodes by reciprocated conformity with the wired networking communications or, perhaps, progress to sovereign networks. However, when we envisage rapid increase in number of Ad Hoc applications relies on a many attributes, with the characteristics of reliability and coherence as key factors to be addressed. Scorn the subsistence of eminent security systems, further vulnerabilities to the position to this new networking pattern cause to be such conventional solution inapt for prevailing conditions. This survey paper eludes the facts and study of the past and most resent research carried out in "Ad hoc network's routing security".

Keywords **:** Ad hoc networks, Attcks, Routing , Security**.**

I. INTRODUCTION

Research on Wireless Ad Hoc Networks is a very interesting phenomenon, as every research is with an outcome of the evaluations, deep insight to the nitty gritty of how the ad hoc networking systems work. When we prelude the previous studies the crux lies in identifying the scope which emerged in to the application usage of the systems and can be termed with the usage from Defense Advanced Research Project Agency (DAPRPA) packet radio networks (PRNet), which evolved into the survivable adaptive radio networks (SURAD) program [1]. Ad hoc networks turn out has a vital ole in applications pertaining to military and its allied research works, for example, the global mobile information systems (GloMo) program and the near-term digital radio (NTDR) program [2]. Recent years have seen a whole new splash of applications in industrial and commercial wireless ad hoc networks, as viable communication equipment and portable computers become more compact and available.

From the time period of its existence in to the applications way back in 1970's, wireless systems kind of networks gained its credibility towards its waving service as they support the mobile users with sound computing facilities and the processing of information system without influence of user's place of contact. These kinds of Ad hoc networks can be identified to infrastructure network and the ones without any assigned infrastructure.

The infrastructure networks have fixed and wired gateways or the fixed Base-Stations which are connected to other Base-Stations through wires. Each node is within the range of a Base-Station. A "Hand-off" is displayed when host of the mobile moves beyond the array of one Base-Station and enters the array of another Base-Station and in this way; mobile host is able to maintain continuity communication seamlessly throughout the network. Example applications of this type include wireless local area networks and Mobile Phone. The other type of wireless network, infrastructure less networks, is knows as Mobile Ad-hoc Networks (MANET). These networks have no fixed routers, routers function can be performed by every node. Every node has the capacity for movement and they can be connected dynamically in arbitrary manner. The terminals are systemized to distribute within the nodes, the tasks of streamlining and monitoring the network communications. As the entire model of this network has the mobility, the independent terminals are positioned to move as needed, thus this kind of system facilitates them to converse with the terminal in range or can opt for an intermediary if the terminals for communication are from the outer range. This kind of networks can be termed as multi-hop or store-and-forward networks. The nodes in these networks can function like routers, which finds out and safeguards other nodes routes present in the networks. The possible locations for these nodes can be on airplanes, ships, trucks, cars, perhaps even on people or very small devices.

Mobile Ad-hoc Networks are supposed to be used for disaster recovery, battlefield communications, and rescue operations when the wired network is not available. It can provide a feasible means for ground communications and information access.

II. OVERVIEW OF ROUTING PROTOCOLS IN AD HOC NETWORKS

Wireless Ad-hoc Networks operates without a fixed infrastructure. Multi-hop, mobility, large network size combined with device heterogeneity and bandwidth and battery power limitations, all these factors make the design of routing protocols a major challenge. Lots of researchers did

tremendous work on the Wireless Ad-hoc Routing Protocols. Two main kinds of Routing Protocols are existed today: one is called table-driven protocols (including distance vector and link state), another is on-demand protocols. [3]

In table driven routing protocols, the protocols consistent and up-to-date routing information to all nodes is maintained at each node whereas in on-demand routing the routes are created only when desired by the source host.

While for the on demand Routing protocols, "on demand" means that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. [4] If we look up the key words "Wireless Ad hoc Networks Routing Protocols" in Google, we could find tons of millions of all kinds of routing protocols, as LAR (Location-Aided Routing), DSDV (Destination-Sequenced Distance-Vector Routing), AODV (Ad-hoc On-Demand Distance Vector Routing), and DSR (Dynamic Source Routing Protocol). However, after survey various types of routing strategies proposed for wireless ad-hoc networks, we find the truth is all these routing protocols are all have inherent drawbacks and cannot be considered as good routing protocols for Wireless ad hoc Networks. Just like Windows operating systems need patch at all the time, the Wireless Ad hoc networks routing protocol are all needs patches too.

The Key issues which are tagged with routing protocols can be attributed to below factors:

[a] At first when we take rapid passing pattern in to the account, it can be coined as to be one node transient through the whole network very quickly. Such a rapid passing node will generate the following affects to the whole network. First, the topology of the network changed rapidly, which will lead to the lost of packets. Second, we have to modify every node's routing table that within the communication distance of the rapid-passing node, that will greatly improve the consumption of the bandwidth and the overhead of the networks. Third, obviously there will be tremendous delay of the data sending to the rapid-moving node.

[b] It can't be escalated as that the communication can happen in the two way process over wireless systems of networks amid two or more hosts. This envisages the crux that few routing protocols which are predetermined to certain routes may not respond in similar kind on an unassigned direction for transmissions.

[c] It could be factored that much of this routes which are created by the routing protocols might also happen to be with uncalled-for routes, which might directly impact the load of the routing updates and the network overload.

Periodically sending routing tables will waste network bandwidth. When the topology changes slowly, sending routing messages will greatly waste the bandwidth of Wireless Ad-hoc Networks. This will add additional burdens to the limited bandwidth of the Ad-hoc Networks.
Periodically sending routing tables also waste the battery power. Energy consumption is also a critical factor which prevents Wireless Ad-hoc Networks to be a non-flowed architecture.

We all understand that a stable network routing protocols is essential for any kinds of networks. Despite of numerous researches taking place in the domain of Wireless ad hoc Networks, hardly any study could find a consistent routing protocol. When we attempt to understand the kinds of routing protocols, it can be classified as two segments one is proactive routing protocols and the other is reactive routing protocols.

A. Proactive Routing Protocols

` This kind of protocols persists its routes to possible destinations, being immaterial about the requirement of such routes or not. Further to create a corrective measure a node has to be timely send the conversant messages to the other nodes, which might result in more bandwidth occupation and other such phenomenal issues. The prima face of these constraints is because of automated with no kind of coherence to the existence of traffic in the destined location. The key advantage of this kind of protocol is that hosts can avail the information pertaining to routes and also to create sessions in quick turnaround time. [5]

To illustrate the proactive routing protocol we can see how the established proactive protocol created by GSR works. When we consider LS routing scenario, all the information pertaining to change in the routes towards nodes will be flooded in to the network as and when any changes are identified in the links amid of themselves and the neighbors. When such a communication passé happens it eludes certain amount of delay towards each of its neighbors. In a system of static topology LS routing can work to the optimum levels, however when link changes frequently it lead to the overload of information system on the networks. When we take in to consideration the GSR model, it will not dwell in to the networks with loads of data, whereas it ensures that every node is maintaining a consistent link table with updates pertaining to the LS data which is received from the other nodes and keep transacting the same information with the other corresponding nodes from the neighborhood. It uses the gamut of sequence number to identify the LS information which is transacted with the corresponding nodes, as this curtails the over load information on the networks. [6]When we consider the Distributed Bellman-Ford (DBF) kind of protocol, the uniting time which is required to track a link in the GSR is quite shorter, as in GSR the peripheral network range of a terminal and the link update level in a frequency is

usually smaller in comparison to the intervals. As the global system structure is maintained at all the nodes, it provides scope for preventing any short come and turns to be hassle free.

The disadvantages with the proactive protocols like GSR are the volume of the update message transmissions systems as it might occupy considerable bandwidth and the covert of LS system of information propagation, as it depends on the update time intervals. A technology termed as "Fish Eye" could be considered in mitigating the volume of the messages for updating, whereas here every node has to maintain a high rate of accuracy in maintaining the data related to the nearby and neighboring nodes, and relatively moderate data about the nodes which are quite a farther range of its network.

B. Reactive Routing Protocols

This kind of protocols are significant for reducing the burden on the routing mechanisms amid of the networks as they don't preamble its attempts in routes where there is absence of any kind of data traffic. This sort of scenario will directly impact the load factor on the network as they induce very little load when compared to the Proactive Routing system of Protocols. This method of routing could be very optimum in a limited resource environment.

[a] Dynamic Source Routing (DSR) :

The Dynamic Source Routing (DSR) protocol uses the source routing approach (every data packet carries the whole path information in its header) to forward packets. Before a source node sends data packets, it must know the total path to the destination. Otherwise, it will initiate a route discovery phase by flooding a Route REQuest (RREQ) message.

As mentioned the RREQ system carries the numbering mechanism thru sequences to the intermediaries it pass through towards the header of the message. This facilitates the system in such a way that once the same header message is received by the other counter nodes too, the broadcasting of the same will be curtailed. Once the message kind of RREQ reaches the destination point of node, it sends across a reply in a route of RREP i.e Route REPly packet to the source, RREP will track the pat information from the obtained route of RREQ packet and enrooted to the origin which turns out to be the destination thru the traversed nodes. Every node will use system of route cache to note the complete route to the requisite destinations. [7] [8].

Message transmissions support the network in the detection of route failure, and will instigate a message in correspondence of the error, which will be sent to the source. In the scenarios where the source and the intermediaries receive the intended message, it do obliterate the paths and its broken links from the cache of its routes. The path calculated in DSR is loop-free since loops can be detected easily and erased by the source routing. A few optimizations are proposed for DSR. For example, a flooded route query can be quenched early by having any non-destination node reply to the query if that node already knows a route to the desired destination; the routes can be refreshed and improved by having nodes promiscuously listen to the conversations between other neighboring nodes.DSR is simple and loop-free.

However, it may waste bandwidth if every data packet carries the entire path information. [8] [7] The response time may be large since the source node must wait for a successful RREP if no routing information to the intended destination is available. In addition, if the destination is unreachable from the source node due to a network partition, the source node will continue to send RREQ messages, possibly congesting the network.

[b] Ad hoc On-Demand Distance Vector (AODV) Routing

Since DSR includes the entire route information in the data packet header, it may waste bandwidth and degrade performance, especially when the data contents in a packet are small. Ad hoc On-Demand Distance Vector (AODV) Routing tries to improve performance by keeping the routing information in each node. The main difference between AODV and DSR is that DSR uses source routing while AODV uses forwarding tables at each node. In AODV, the route is calculated hop by hop. Therefore, the data packet need not include the total path. [9]

The route discovery mechanism in AODV is very similar to that in DSR. In AODV, any node will establish a reverse path pointing toward the source when it receives an RREQ packet. When the desired destination or an intermediate node has a fresh route (based on the destination sequence number) to the destination, the destination/intermediate node responds by sending a route reply (RREP) packet back to the source node using the reverse path established when the RREQ was forwarded. [9] .When a node receives the RREP; it establishes a forward path pointing to the destination. It tracks and records the path from the exhibited source to the intended destination when a successful message of deliver is responded by RREP.
AODV saves bandwidth and performs well in a large MANET since a data packet does not carry the whole path information. As in DSR, the response time may be large if the source node's routing table has no entry to the destination and thus must discover a path before message transmission. Furthermore, the same problems exist as in DSR when network partitions occur.

C. Hybrid Routing Protocols

A typical hybrid routing protocol is Zone Based Routing (ZBR). ZBR combines the Proactive and reactive routing approaches. It divides the network into routing zones. The

Routing zone of a node X includes all nodes within hop distance at most d from node X.

All nodes at hop distance exactly d are said to be the peripheral nodes of node X's routing zone. The parameter d is the zone radius. ZBR proactively maintains the routes within the routing zones and reactively searches for routes to destinations beyond a node's routing zone. Route discovery is similar to that in DSR with the difference that route requests are propagated only via peripheral nodes. ZBR can be dynamically configured to a particular network through adjustment of the parameter.ZBR will be a purely reactive routing protocol when d = 0 and a purely proactive routing protocol when d is set to the diameter of the network.ZBR discovers routes as follows. When a source node wants to send data to a destination, it first checks whether or not the destination is within its routing zone. If it is, then a route can be obtained directly. Otherwise, it floods a route request to its peripheral nodes. The peripheral nodes in turn execute the same algorithm to check whether the destination is within their routing zone. If it is, a route reply message is sent back to the source. Otherwise, the peripheral node floods the route request to its peripheral nodes again. This procedure is repeated until a route is found.

III. PROACTIVE vs REACTIVE vs HYBRID PROTOCOLS

The tradeoffs between proactive and reactive routing strategies are quite complex. Which approach is better depends on many factors, such as the size of the network, the mobility, the data traffic and so on. Proactive routing protocols try to maintain routes to all possible destinations, regardless of whether or not they are needed. [11]

In proactive nature of routing protocols the information is continuously disseminated and recorded for updates. Where as in the reactive nature of routing system protocols only when the data traffic is encountered the protocols instigate in the desired route location. This pedagogy can drastically curtail the load factors on the network protocol prevails the conditions of static nature and also on lighter traffic scenarios. [10]

The hybrid routing approach can adjust its routing strategies according to a network's characteristics and thus provides an attractive method for routing in MANETs. However, a network's characteristics, such as the mobility pattern and the traffic pattern, can be expected to be dynamic. The related information is very difficult to obtain and maintain. This complexity makes dynamically adjusting routing strategies hard to implement.

IV SECURITY IN WIRELESS AD HOC NETWORKS

Security is an important thing for all kinds of networks including the Wireless Ad Hoc Networks. It is obviously to see that the security issues for Wireless Ad Hoc Networks are difficult than the ones for fixed networks. This is due to system constraints in mobile devices as well as frequent topology changes in the Wireless networks. Here, system constraints include low-power, small memory and bandwidth, and low battery power.Mobility of relaying nodes and the fragility or routes turn Wireless Ad-hoc Network architecture into highly hazardous architectures. No entity is ensured to be present at every time and it is then impossible to rely on a centralized architecture that could realize network structure or even authentication. The people who consider the Mobile Ad hoc Networks are not a flawed architecture, while we cannot see it used in practice is only because most of its applications are in military are totally wrong. It is true that Mobile Ad hoc Networks come from the military. But perhaps those persons forgot one of the most important things: the Security.Everybody knows that the core requirement for military applications dealing with trust and security! That is to say, security is the most important issue for ad hoc networks, especially for those security sensitive applications.

As we have mentioned before, in Mobile Ad- hoc Networks, security is difficult to implement because of the networks constrains and the rapidly topology changes. After investigation, we found that there are two kinds of security related problems in the Mobile Ad-hoc Networks.One is the attacks based on the networks which are just similar to the Internet, the other is Fault Diagnoses.Fault Diagnoses algorithm is used to pick out the faulty nodes and at the same time remove the node from the whole networks. This process should be real-time as to guarantee the performance of the whole networks. In order to solve the fault diagnoses problem, many fault diagnoses algorithms [13] were bring out. After carefully surveying the existing algorithm today, we found that they cannot correctly diagnose faulty node with the presence of the changing of the network topology during the process of diagnosis, and these algorithms are analyzed with repetitious diagnosis for all the mobile hosts and cause the great system overhead due to the transmission of diagnosis messages by means of flooding throughout the whole networks. While the topology of Mobile Ad-hoc Networks changes from time to time, then we cannot use this kind of Fault Diagnoses Algorithm to solve the questions. Therefore, we can see that the current fault diagnosis algorithms cannot solve the fault diagnosis problem [12]As for the networks attacks, there are several factors of security that we should consider. First, *Availability* ensures the

survivability of network services despite denial of service attacks. And the other crucial factor is the matter of Confidentiality as the routing protocol has to be secured and ensures no unauthorized entities are provided with the access, factored to the integrity as to make sure that the message is transmitted to the destination without any corrupt in the message system. Authentication suffices the node with the identity of the neighbor node which is intended to communicate with in a systematic manner. However structured the secure network is, still there is scope for the adversary to erase the messages, append it and also at times might masquerade a node by violating all the principles of the application systems like authentication, coherence to the destination etc. [13] [14] .Despite the repeated researches to address these issues, not much of success is envisaged in this front as the routing protocols are still vulnerable to the security attacks, in the ad hoc networks. While, on the other hand, it is said that the main applications of MANET are in military and emergency, all these applications are security-sensitive. MENAT can not satisfy the security requirement of the applications, so this makes that MANET is a flawed architecture.

V. SECURITY ATTACKS IN AD HOC WIRELESS NETWORKS

Wireless mobile ad hoc nature of MANET brings new security challenge to the network design. Mobile wireless networks are generally more vulnerable to information and physical security threats than wired networks. Vulnerability of channels and nodes, absence of infrastructure and dynamically changing topology, make ad hoc networks security a difficult task.In the case of broadcast wireless systems, channels allow the scope for tamper of message and also at times injection. These conditions prevail as the nodes are not present in secured places and can easily be prey to the attacker's around the corner. Lack of any structured infrastructure creates the need for robust security solutions as the issue of online server security protocol networks is inapplicable. In the given constraint it is turning out to be very apprehensive towards aiming a secured wireless ad hoc network routing protocols.

Understanding possible form of attacks is always the first step towards developing good security solutions. Ad hoc networks have to cope with the same kinds of vulnerabilities as their wired counterparts, as well as with new vulnerabilities specific to the ad hoc context. Furthermore, traditional vulnerabilities are also accentuated by the ad hoc paradigm. [15] Below we summarize only the main directions of security in ad hoc networks. Performing communication in free space exposes ad hoc networks to attacks as anyone can join the network, and eavesdrop or inject messages. Ad hoc networks attacks can be classified as passive or active. Passive attack signifies that the attacker does not send any message, but just listens to the channel. A passive attack does not disrupt the operation of a protocol, but only attempts to discover valuable information.

During an active attack, on the other hand, information is inserted into the network. Passive eavesdropping is a passive attack that attempts to discover nodes information by listening to routing traffic. In a wireless environment it is usually impossible to detect this attack, as it does not produce any new traffic in the network. Active attacks involve actions such as the replication, modification and deletion of exchanged data. Certain active attacks can be easily performed against an ad hoc network. These attacks can be grouped in: Impersonation, Denial of service, and Disclosure attack. [15]

A. *Impersonation* :

In this type of attack, nodes may be able to join the network undetectably, or send false routing information, masquerading as some other trusted node. The Black Hole attack falls in this category: here a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. A more subtle type of routing disruption is the creation of a tunnel in the network between two colluding malicious nodes.[16]

B. Denial of service:

The Routing Table Overflow and the Sleep Deprivation attacks fall in this category. In the former, the attacker attempts to create routes to non-existent nodes to overwhelm the routing-protocol implementations In the latter, the attacker attempts to consume batteries of other nodes by requesting routes, or by forwarding unnecessary packets.

C. Disclosure attack :

A location disclosure attack can reveal something about the physical location of nodes or the structure of the network. Two types of security mechanisms can generally be applied: preventive and detective. Preventive mechanisms are typically based on key-based cryptography. Keys distribution is therefore at the center of these mechanisms. Secret keys are distributed through a pre-established secure channel, and this makes symmetric cryptography generally difficult to apply in ad hoc networks.[15][16]Public keys are distributed through certificates that bind a public key to a device. In the centralized approach, certificates are provided, stored, and distributed by the Certificate Authority. Since no central authority, no centralized trusted third party, and no central server are possible in MANET, the key management function needs to be distributed over nodes. The key management responsibility is shared among a set of nodes, called servers. The challenge of constructing such a trustworthy aggregation lies not only in how to create and configure the aggregation, but also in how the aggregation maintains its security by

adapting to changes in the network topology. . In this approach the users issue certificates for each other based on their personal acq uaintances.

In ad hoc network there are no traffic concentration points, where the intrusion detection system (IDS) can collect audit data for the entire network. The typical adjudge factors will be constrained to the radio range and the detection mechanisms of the designed algorithms which usually rely on the fractional and the divisional information source. Ad-hoc networks will not possess any explicit infrastructure. In this kind of system it is a temporary network which is created for the users and it doesn't demand any centralized administration.

When the mobile scope of the user is tagged to the ad-hoc network they had created its structure dynamically, as it supports all the mobile nodes for the scope of routing. When the medium of wireless applications are considered the issues of limitations pertaining to the range of transmission will hamper the communication process without the use of the intermediaries. Previously many routing protocols has been proposed to this kind of changing network structure management as they could mitigate the usage of resources like bandwidth, and the system usage to a considerable levels. When we consider the usage of defense and the other security sensitive operations, the trend is towards creating the usage of ad hoc networks because of their unique features. One of the key issues which are identified with the design process of this sort of networks is their weak structure for the security networks. [17]

One more hurdle which is faced with routing protocol mechanisms is that when we have numerous nodes to get connected in the communication network, for an instance to establish connection from one node to the other farthest node in the topology, it requires a very robust and systematic approach which can track the shortest possible route. This is enabled with the four major routing protocols which are inducted in to the application levels intended for the above mentioned issue. [17]

The four Major Routing Protocols which could support the quantitative requirements are as follows:

[a] Temporally Ordered Routing Algorithm (TORA)
[b] Ad Hoc on Demand Distance Vector (AODV)
[c] Dynamic Source Routing (DSR)
[d] Destination Sequenced Distance Vector (DSDV)

Challenges Traditional security mechanisms, such as authentication protocols, digital signature, and encryption, still play important roles in achieving confidentiality, integrity, authentication, and non-repudiation of communication in ad hoc networks. However, these mechanisms are not sufficient by themselves. When we take in to consideration the features of ad hoc networks it eludes wide scope of feasibilities to overcome the hurdles pertaining to the security factors, the use of wireless links probe to ad hoc network which can find susceptible link of attacks of all kinds as discussed in the earlier sections. In the purview of the same, it's not that one has to consider the possible attacks from the outer range of the network, where as one has to mind the attacks which could be launched from within the network too by the compromised nodes. Hence in order to achieve high survivability, ad hoc networks has to have a distributed topology without having any central entities as any such central entity might be vulnerable state for the entire protocol network.

In lieu to curtail the attacks on the routing protocols of the ad hoc networks, heading to a static configuration alone would not resolve the issue, and hence the security mechanisms should be scalable to manage a huge network too without any interruptions. [17]

Confidentiality is also the crucial factors as all queries and neighborhood discoveries are done, trusting whomever the routing protocol talks to. There are no authentication methods embedded in routing protocols, except IMEP.

VI. SECURITY MECHAQNISMS AND SOLUTIONS IN WIRELESS NETWORKS

Several routing protocols have been proposed for routing in ad hoc networks; however, until recently, security in such networks has not yet enjoyed much attention from the research community. As a result, ad hoc network routing protocols that assume a trusted environment are highly vulnerable to attack; for example using the wormhole or rushing attacks, an adversary can paralyze ad hoc networks. Few of the efficient applications which can enact as a security mechanism to the routing protocols and create a robust system to withstand vulnerable attacks are in place and few of them are Ariadne, SEAD, and RAP and also few other security protocols [18]

A. *Ariadne*

In this research project, we present attacks against routing in ad hoc networks, and we present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne. It restricts attackers and other nodes which are vulnerable from with in the network also from corrupt with active routes, and also avert various kinds of Denial-of-Service kind of attacks too. [18] [19]

B. *Sead*

Although many previous ad hoc network routing protocols have been based in part on distance vector approaches, they have generally assumed a trusted environment. In this research project, we design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV). In order to support use with nodes of limited CPU processing capability, and to guard against

Denial-of-Service (DoS) attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol.[21] SEAD performs well over the range of scenarios we tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.[20]

VII. RAP SECURE AD-HOC NETWORK ROUTING PROTOCOL

Many proposed routing protocols for ad hoc networks operate in an on-demand fashion, as on-demand routing protocols have been shown to often have lower overhead and faster reaction time than other types of routing based on periodic (proactive) mechanisms. Significant attention recently has been devoted to developing secure routing protocols for ad hoc networks, including a number of secure on-demand routing protocols, that defend against a variety of possible attacks on network routing. In this research project, we present the rushing attack, a new attack that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. This attack is also particularly damaging because it can be performed by a relatively weak attacker. We analyze why previous protocols fail under this attack. We then develop Rushing Attack Prevention (RAP), a generic defense against the rushing attack for on-demand protocols. RAP incurs no cost unless the underlying protocol fails to find a working route, and it provides provable security properties even against the strongest rushing attackers. [22]

There is many more such kind of security mechanisms which can ensure that the routing protocol of the security network is secured and can deliver the intended operations for which it has been intended too.

VIII. REFERENCES

[1] J. A. Freebersyser and B. Leinerr, "A DoD perspective on mobile ad hoc networks," in Ad Hoc Networking, C. E. Perkin,Ed. Addison-Wesley, 2001, pp. 29–51.

[2] B. Leiner, R. Ruth, and A. R. Sastry, "Goals and challenges of the DARPA GloMo program," IEEE Personal Communications, vol. 3, no. 6, pp. 34–43, December 1996

[3] M. Haardt W. Mohr R. Becher, M. Dillinger. Broadband wireless access and future communication networks. proceedings of the IEEE, 89(1), 2001

[4] David B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts", Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, December 1994.

[5] Y. -C. Hu, D. B. Johnson and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Fourth IEEE Workshop on Mobile Computing Systems and Applications (WM- CSA'02), Jun. 2002.

[6] T. H. Clausen, G. Hansen, L. Christensen, and G. Behrmann, The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation, Proc. of IEEE Symp. on Wireless Personal Mobile Communications 2001, Sep. 2001.

[7] D. B. Johnson and D. A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, Kluwer Academic Publishers, Vol 353, pp. 153-181.

[8] C. E. Perkins and P. Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, SIGCOMM'94 Conf. on Communications architectures, Protocols and Applications,

[9] V. D. Park and M. S. Corson, A Highly Adaptive Distributed Routing Algorithm for MobileWireless Networks, IEEE Infocom 1997, Apr. 1997, pp. 1405-1413.

[10] P. Sinha, R. Sivakumar, and V. Bharghavan, CEDAR: A Core Extraction Distributed Ad Hoc Routing Algorithm, IEEE Journal On Selected Areas in Communications, Vol 17,

[11] Z. J. Haas, The Routing Algorithm for the Reconfigurable Wireless Net- works, Proc. of ICUPC 1997, Vol 2, Oct. 1997, pp. 562-566.

[12] S.Chessa, P.Santi, "Comparison Based System-Level Fault Diagnosis in Ad-Hoc Networks", Proc. IEEE 20th Symp. on Reliable Distributed Systems (SRDS), New Orleans, pp. 257-266, October 2001

[13] D. Coppersmith and M. Jakobsson, Almost Optimal Hash Sequence Traversal, In Proc. of The Sixth Intl. Conf. on Financial Cryptography (FC 2002), Lecture Notes in Computer Science, Springer 2002. [5] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks, ACM CCS 2003, Oct. 2003, pp. 42-51

[14] D. B. Johnson and D. A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, Kluwer Academic Publishers, Vol 353, pp. 153-181.

[15] C. Jones, K. Sivalingam, P. Agarwal, J.C. Chen, A survey of energy e.cient network protocols for wireless and mobile networks, ACM/Kluwer Wireless Networks 7 (4) (2001) 343–358.

[16] Eun-Sun Jung, Nitin H. Vaidya, A power control MAC protocol for ad hoc networks, in: Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking

[17] Security Challenges for Routing Protocol in AD-HOC Networks. International Journal of Applied Engineering Research, 2008by V. Kamakshi Prasad, C. Raghavendra Rao, P. V. S. Srinivas

[18] Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks." InWireless Networks Journal, 11(1), 2005.[PDF]

[19] Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks." InProceedings of the Eighth Annual International Conference on Mobile Computing and Networking (ACM Mobicom), Atlanta, Georgia, September 23 - 28, 2002. [PDF]

[20] Hu, Yih-Chun, Dave Johnson, and Adrian Perrig. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks." In Ad Hoc Networks Journal, 1(1):175-192, 2003. [PDF]

[21] Hu, Yih-Chun, Dave Johnson, and Adrian Perrig. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks." In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), June 2002.[PDF]

[22] Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols." In Proceedings of the ACM Workshop on Wireless Security (WiSe), San Diego, California, September 2003.[PDF]