**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 3, Issue. 9, September 2014, pg.646 – 655*

**RESEARCH ARTICLE**

# A SECURE AND ENERGY EFFICIENT APPROACH IN ADHOC NETWORKING

**Manisha.K**[1]
M.Tech Student
Dept. of IT
SNIST, Hyderabad
manisha.kalyani@yahoo.com

**Sunil Bhutada**[2]
Associate Professor
Dept. of IT
SNIST, Hyderabad
sunilbhutada@gmail.com

***Abstract*— *An Ad-Hoc network is collection of wireless mobile nodes forming a temporary network without the use of any established infrastructure or fixed centralized administration. In Ad-Hoc networks the communicating nodes do not depend on a fixed infrastructure, which sets a new challenge for the necessary security architecture which they apply. In such an environment, it is necessary for one mobile node to enlist the use of other nodes in forwarding a packet to the destination, due to the limited range of bandwidth and signals of each mobile node wireless transmission. Movement of the nodes results in a change in routing paths, which requires some secure mechanisms for determining new routing paths. The deployment of sensor networks in security and safely critical environments requires secure communication primitives. Sensor networks in hostile environment make it vulnerable to the battery power drainage attacks. It is impossible to replace or recharge the battery power of the sensor nodes. Among different types of security attacks, low power sensor nodes are immensely affected by the attacks which cause random drainage of the energy level of sensors, leading to death of the nodes. In this paper we present secure routing protocols in Ad-Hoc networks to overcome this type of attacks.***

***Keywords*— *Ad-Hoc network, Routing, Power draining, Mobile nodes, Sensor nodes***

## I. INTRODUCTION

Number of factors associated with regulation, social behaviour, technology and business naturally and logically speaks in the favour of wireless Ad-Hoc networking. Ad-Hoc network communication, which is advancing in both terms of usage and technology and is a driving force, thanks to Internet and second-generation cellular systems. As we look at horizon, we can have a glimpse of truly ubiquitous computing and communication. In the future, the role and the capabilities of short-range data transactions are to be expected to grow, which serves as a complement to the traditional large-scale communication. Most of the man made

 

machine communication as well as oral communication between human to human occurs at distances of less than 10M also, as a result of this type of communication, the two communicating parties very often have need to exchange data. As an empowering factor, a license-exempted frequency band invites the use of developing the radio technologies (such as Bluetooth) that admit effortless and inexpensive deployment of the wireless communication. In terms of usability, portability, price and in context of an Ad-Hoc network, many of the computing and communication devices, like PDA and mobile phones, which already possess attributes that are desirable.

Mobile hosts and the wireless networking hardware's are becoming widely available to all, and large-scale work has been done recently in collaborating these elements into the traditional networks such as Internet. Sometimes, mobile users want to communicate in some situations where there is no fixed wired infrastructure, because it might not be physically possible or economically practical to provide the required infrastructure or because of the convenience of the situation does not permit the infrastructure installations. For instance, class students may require interacting during a lecture, friends or some business associates may run into each other in an airport terminal/some place where there is no infrastructure and they wish to share some important files. In such type of situations, a collection of mobile nodes with wireless network interfaces may form a temporary network without the requirement of any centralized administration or established infrastructure. This type of wireless network is known as an Ad-Hoc network.

Fig. 1 Architecture of Ad-Hoc network

An Ad-Hoc network as shown in Fig.1 is a collection of mobile nodes that do not depend on a predefined infrastructure to keep the network connected. In an Ad-Hoc network, there is no fixed infrastructure like base stations or MSC (mobile switching centers). Mobile nodes which are within each other's radio range can communicate directly using wireless links, while those which are far away depend on other nodes to replay message packets as routers. Frequent changes of the network topology occur in an Ad-Hoc network due to the node mobility. Nodes of an Ad-Hoc network are mostly mobile in nature, which also shows that they apply wireless communication to maintain the connectivity in between them, in this case the networks are called as mobile Ad-Hoc networks (MANET). Node mobility in an Ad-Hoc network causes frequent changes of the network topology.

The IEEE 802.11 technology is a very good platform to execute Single-Hop Ad-Hoc networks because of the extreme simplicity of the network. Single-hop means the nodes in the network must be within the same transmission range (say 200-300 meters) to communicate. This type of limitation can be overcome by Multi-Hop Ad-Hoc networking. This requires the additional routing mechanisms at nodes so to forward packets towards the required destination, which extends the range of Ad-Hoc network beyond the transmission range of the source node. Routing mechanisms designed for wired networks are not suitable for the Ad-Hoc network environment, due to the dynamic topology of Ad-Hoc networks.

Ad-Hoc networks can be very different from each other, depending on the type and the area of application. For example in a computer classroom an Ad-Hoc network can be formed in between students PDAs and the

 

workstation of the teachers, a group of soldiers operating in a hostile environment, trying to keep their presence and mission totally secure and unknown from the viewpoint of enemy. These two scenarios of Ad-Hoc networking are very different from each other in many ways in the first scenario the mobile devices need to work in a friendly and safe environment where the networking conditions can be predictable. Thus no special security requirements are needed. On the other hand, the devices are required to operate in an extremely hostile, secured and demanding environment, in this case the protection of the communication and the mere availability and operation of the network are both very vulnerable without strong protection.

Wireless Ad-Hoc networks have matured as a viable means to provide ubiquitous untethered communication. In order to enhance network connectivity, a source communicates with far off destinations by using intermediate nodes as relays [1], [2], [3], [4]. However, the limitation of finite energy supply raises concerns about the traditional belief that nodes in Ad-Hoc networks will always relay packets for each other. Consider a user in a campus environment equipped with a laptop. As part of his daily activity, the user may participate in different Ad-Hoc networks in classrooms, the library and coffee shops. He might expect that his battery-powered laptop will last without recharging until the end of the day. When he participates in these different Ad-Hoc networks, he will be expected to relay traffic for other users. If he accepts all relay requests, he might run out of energy prematurely. Therefore, to extend his lifetime, he might decide to reject all relay requests. If every user argues in this fashion, then the throughput that each user receives will drop dramatically. We can see that there is a trade-off between an individual user's lifetime and throughput. Cooperation among nodes in an Ad-Hoc network has been previously addressed in [5], [6], [7], [8], [9]. In [5], nodes, which agree to relay traffic but do not, are termed as misbehaving. Clever means to identify misbehaving users and avoid routing through these nodes are proposed. Their approach consists of two applications: Watchdog and Pathrater. The former runs on every node keeping track of how the other nodes behave; the latter uses this information to calculate the route with the highest reliability.

In this paper we focus on secure routing and also an important factor power saving of nodes in a network. This power draining from nodes is the latest research area now-a-days. We try to form a secure routing path which takes less time and less energy to transfer the data packets.

## II. RELATED WORK

Secure routing in networks such as the Internet has been extensively studied [10, 11, 12, 13, 14, 15]. Many proposed approaches are also applicable to secure routing in Ad-Hoc networks. To deal with external attacks, standard schemes such as digital signatures to protect information authenticity and integrity have been considered. For example, Sirios and Kent [14] propose the use of a keyed one-way hash function with windowed sequence number for data integrity in point-to-point communication and the use of digital signatures to protect messages sent to multiple destinations.

Perlman [10] studies how to protect routing information from compromised routers in the context of Byzantine robustness. The study analyzes the theoretical feasibility of maintaining network connectivity under such assumptions. Kumar [12] recognizes the problem of compromised routers as a hard problem, but provides no solution. Other works [13, 14, 15] give only partial solutions. The basic idea underlying these solutions is to detect inconsistency using redundant information and to isolate compromised routers. For example, in [15], where methods to secure distance-vector routing protocols are proposed, extra information of a predecessor in a path to a destination is added into each entry in the routing table. Using this piece of information, a path-traversal technique (by following the predecessor link) can be used to verify the correctness of a path. Such mechanisms usually come with a high cost and are avoided (e.g., in [13]) because routers on networks such as the Internet are usually well protected and rarely compromised.

Because routing is an important problem in mobile Ad-Hoc networks, researchers have explored many routing protocols for this environment, many based on, or developed as a part of, work produced by early DARPA packet-radio programs such as PRNet [16], and SURAN [17]. Recently, some researchers have considered the performance of TCP on multi-hop networks [18, 17]. Gerla et al. [17] investigated the impact of the MAC protocol on performance of TCP on multi-hop networks. Chandran et al. [18] proposed the TCP-Feedback (TCP-F) protocol, which uses explicit feedback in the form of route failure and reestablishment

 

control packets. Performance measurements were based on a simple one-hop network, in which the link between the sender and receiver failed/recovered according to an exponential model. Also, the routing protocol was not simulated.

Durst et al. [19] looked at the Space Communications Protocol Specifications (SCPS), which are a suite of protocols designed by the Consultative Committee for Space Data Systems (CCSDS) for satellite communications. SCPS-TP ANALYSIS OF TCP PERFORMANCE OVER MOBILE AD-HOC NETWORKS 287 handles link failures using explicit feedback in the form of SCPS Control Message Protocol messages to suspend and resume a TCP sender during route failure and recovery. Performance measurements focused on link asymmetry and corruption over last-hop wireless networks, common in satellite communications.

Design of routing protocols is a crucial problem in mobile Ad-Hoc networks [20], and several routing algorithms have been developed. One desirable qualitative property of a routing protocol is that it should adapt to the traffic patterns. Johnson and Maltz [21] point out those conventional routing protocols are insufficient for Ad-Hoc networks, since the amount of routing related traffic may waste a large portion of the wireless bandwidth, especially for protocols that use periodic updates of routing tables. They proposed using Dynamic Source Routing (DSR), which is based on on-demand route discovery. A number of protocol optimizations are also proposed to reduce the route discovery overhead. Perkins and Royer [22] present the AODV (Ad-Hoc On demand Distance Vector routing) protocol that also uses a demand-driven route establishment procedure. TORA (Temporally-Ordered Routing Algorithm) [23] is designed to minimize reaction to topological changes by localizing routing-related messages to a small set of nodes near the change. Hass and Pearlman [24] attempt to combine proactive and reactive approaches in the Zone Routing Protocol (ZRP), by initiating route discovery phase on demand, but limiting the scope of the proactive procedure only to the initiator's local neighbourhood. Recent papers present comparative performance evaluation of several routing protocols.

A particular problem with the use of distance vector routing protocols in networks with hosts that move, is the possibility of forming routing loops. In order to eliminate this possibility, Perkins and Bhagwat have recently proposed adding sequence numbers to routing updates in their Destination-Sequenced Distance Vector (DSDV) protocol [25]. These sequence numbers are used to compare the age of information in a routing update, and allow each node to preferentially select routes based on the freshest information. DSDV also uses triggered routing updates to speed route convergence. In order to damp route fluctuation and reduce congestion from large numbers of triggered updates after a route changes, each node in DSDV maintains information about the frequency with which it sees route changes and may delay some routing updates.

The Internet Address Resolution Protocol (ARP) is used to find the MAC address of a host on the same LAN as the sender. ARP is somewhat similar to our non propagating route request packets, except that a mobile host may answer the route request from its cache whereas ARP requests are normally only answered by the target host itself. In cases in which several LANs have been bridged together, the bridge may run "proxy" ARP [24], which allows the bridge to answer an ARP request on behalf of another host. In this sense, our non propagating route requests are also similar to proxy ARP in that they expand the effective size of a single host's route cache by allowing it to cheaply make use of the caches of neighbouring hosts to reduce the need for propagating request packets.

## III. SECURE ROUTING

To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. Routing protocols proposed for Ad-Hoc networks cope well with the dynamically changing topology. However, none of them, to our knowledge, have accommodated mechanisms to defend against malicious attacks. Routing protocols for Ad-Hoc networks are still under active research. There is no single standard routing protocol. Therefore, we aim to capture the common security threats and to provide guidelines to secure routing protocols. In most routing protocols, routers exchange information on the topology of the network in order to establish routes between nodes. Such information could become a target for malicious adversaries who intend to bring the network down.

In below sections we can see two secured routing protocols for Ad-Hoc networks to overcome the security attacks and power draining attacks.

 

*A. Clean-Slate Sensor Network Routing*

In this section we show that a clean-slate secure sensor network routing protocol by Parno, Luk, Gaustad, and Perrig ("PLGP" from here on) [26] can be modified to provably resist attacks during the packet forwarding phase. The original version of the protocol, although designed for security, is vulnerable to attacks. PLGP consists of a topology discovery phase, followed by a packet forwarding phase, with the former optionally repeated on a fixed schedule to ensure that topology information stays current. (There is no on-demand discovery.) Discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme. When discovery begins, each node has a limited view of the network — the node knows only itself. Nodes discover their neighbours using local broadcast, and form ever-expanding "neighbourhoods," stopping when the entire network is a single group. Throughout this process, nodes build a tree of neighbour relationships and group membership that will later be used for addressing and routing. At the end of discovery, each node should compute the same address tree as other nodes. All leaf nodes in the tree are physical nodes in the network, and their virtual addresses correspond to their position in the tree (see Fig.2). All nodes learn each others' virtual addresses and cryptographic keys. The final address tree is verifiable after network convergence, and all forwarding decisions can be independently verified.

Furthermore, assuming each legitimate network node has a unique certificate of membership (assigned before network deployment), nodes who attempt to join multiple groups, produce clones of themselves in multiple locations, or otherwise cheat during discovery can be identified and evicted.

*1) Topology Discovery:*

Discovery begins with a time-limited period during which every node must announce its presence by broadcasting a certificate of identity, including its public key (from now on referred to as node ID), signed by a trusted offline authority. Each node starts as its own group of size one, with a virtual address 0. Nodes who overhear presence broadcasts form groups with their neighbours. When two individual nodes (each with an initial address 0) form a group of size two, one of them takes the address 0, and the other becomes 1. Groups merge preferentially with the smallest neighbouring group, which may be a single node. We may think of groups acting as individual nodes, with decisions made using secure multiparty computation. Like individual nodes, each group will initially choose a group address 0, and will choose 0 or 1 when merging with another group. Each group member pretends the group address to their own address, e.g. node 0 in group 0 becomes 0.0, node 0 in group 1 becomes 1.0, and so on. Each time two groups merge, the address of each node is lengthened by one bit. Implicitly, this forms a binary tree of all addresses in the network, with node addresses as leaved.

Note that this tree is not a virtual coordinate system, as the only information coded by the tree are neighbour relationships among nodes. Nodes will request to join with the smallest group in their vicinity, with ties broken by group Ids, which are computed cooperatively by the entire group as a deterministic function of individual member Ids. When larger groups merge, they both broadcast their group Ids (and the Ids of all group members) to each other, and proceed with a merge protocol identical to the two-node case. Groups that have grown large enough that some members are not within radio range of other groups will communicate through "gateway nodes," which are within range of both groups. Each node stores the identity of one or more nodes through which it heard an announcement that another group exists. That node may have itself heard the information second-hand, so every node within a group will end up with a next-hop path to every other group, as in distance-vector. Topology discovery proceeds in this manner until all network nodes are members of a single group. By the end of topology discovery, each node learns every other node's virtual address, public key, and certificate, since every group members knows the identities of all other group members and the network converges to a single group.

*2) Packet Forwarding:*

During the forwarding phase, all decisions are made independently by each node. When receiving a packet, a node determines the next hop by finding the most significant bit of its address that differs from the message originator's address (see Fig.2). Thus every forwarding event (except when a packet is moving within a group in order to reach a gateway node to proceed to the next group) shortens the logical distance to the

 

destination, since node addresses should be strictly closer to the destination (see Fig.2) The final address tree for a fully-converged 6-node network. Leaves represent physical nodes, connected with solid lines if within radio range. The dashed line is the progress of a message through the network. Note that non-leaf nodes are not physical nodes but rather logical group identifiers.

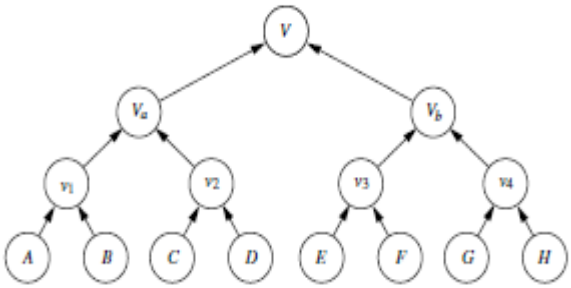


Fig. 2 The final address tree for a fully-converged 6-node network. Leaves represent physical nodes, connected with solid lines if within radio range. The dashed line is the progress of a message through the network. Note that non-leaf nodes are not physical nodes but rather logical group identifiers.

```
Function forward packet(x)
z ← ext_source_add(x);
c ← closest_next_node(z);
if is neighbor(c) then forward(x, c);
else
r ← next_hop_to_non_neighbor(c);
forward(x, r);

Function secure_forward_packet(x);
z ← ext_source_add(x);
a ← ext_attestation(x);
if (not verify_source_sig(x)) or (empty(a) and not is neighbor(z)) or (not saowf_verify(a))
then return; /*drop(x)*/
for each node in a do
prevnode ← node;
if (not are neighbors(node, prevnode)) or (not making progress(prevnode, node))
then return; /*drop(x)*/
c ← closest_next_node(z);
p′ ← saowf_append(x);
if is_neighbor(c) then forward(p′, c);
else forward(p′,next_hop_to_non_neighbor(c));
```

### *B. AODV For Load Balancing*

In Ad-Hoc On-Demand Distance Vector (AODV) routing protocol the network traffic is evenly distributed by using the information available in the network. The basic idea is to select a routing path that consists of nodes with higher energy and hence longer life in order to reduce the routing overhead and end-to-end delay by distributing the packets over the path which is less utilized. The route determining parameters used in our modifications are defined as follows

 

- Route Energy (RE): The route energy is the sum of energy possessed by nodes falling on a route. Higher the route energy, lesser is the probability of route failure due to exhausted nodes.
- Aggregate Interface Queue Length (AIQL): The sum of interface queue lengths of all the intermediate nodes from the source node to the current node.
- Hop count (HC): The HC is the number of hops for a feasible path.

The routing process involved in any routing protocol can be classified in to three main divisions 1.Route Discovery 2.Route Selection 3.Route Maintenance. For implementing our load balancing features effectively in AODV we modified the Route Discovery and Route Selection process.

*1) Route Discovery:*

The route discovery procedure is similar to that of Ad-Hoc On-demand Distance Vector (AODV) routing protocol. Whenever a node wants to send data packets to other node and if there is no route available for that destination node in the routing table, the source node initiates route discovery by broadcasting RREQ (Route Request) packet to all of its neighboring nodes [27]. After receiving the RREQ packet all nodes ensures whether there is a reverse route for that source node if there is no reverse route available in the routing table they update the reverse route to the corresponding source node in their route table. Then if it is the destination node it can send the RREP packet to the source node in the same reverse route. If it is not the destination node it simply forwards the RREQ packet towards the destination node even though they may have route information in their routing table for that destination node. The destination will receive multiple copies of the RREQ packets and each of these RREQ packets will arrive at destination after traveling in different route paths. The destination node responds to all the RREQ packets by sending the RREP packets to each of them in the same path in which the corresponding RREQ packets reached the destination node.

Normally in AODV the RREP packet will contain information like HOP Count, Sequence number but in our modified AODV to better distribute the traffic load evenly we added two more information and they are Route Remaining Energy and Aggregate Interface Queue length in the route path. Initially the destination node adds its Remaining Energy and Queue length and then forwards the RREP to the next intermediate node in the reverse path. When the RREP packets reach the intermediate nodes it sums up their Remaining Energy and queue length. Finally when the RREP packet reaches the source node it contains the sum of the Remaining energy and the total data packets waiting in the queue of the intermediate nodes along the route path in which the RREP packets arrived the source node.

**Algorithm 1** [Route discovery process]

Source node Ns wants to find a path to destination node Nd. Suppose that z is the number of mobile nodes and N is the set of mobile nodes, i.e., N = {N1, N2, . . . , Nz}, where Ns, Ni, Nd ε N, $1 \leq s, d, i \leq z$ and $s \neq d$. We assume that node Ni is an intermediate node that receives the RREQ packet. **If** (node Ni is the destination node Nd) {

4. Destination node Nd adds its remaining energy (RE), aggregate interface queue length (AIQL), and hop count (HC) to the RREP packet.
5. Destination node Nd forwards the RREP packet towards the source node along the path in which the RREQ packet arrived the destination node.
6. Destination node sends reply for each RREQ packet arriving at the destination node after traveling different route path.
7. The intermediate node forwards the route reply towards the source node Ns.

} **else** Node Ni forwards the RREQ packet to the neighbouring node.

*2) Route Selection*

After receiving all the route RREP packets the source node then computes the weight value for each route. Weight for a route i is calculated based on the following:

**$W_i = C1 * (REi/MaxRE) + C2 * (AIQLi/MaxAIQl) + C3* (HCi/MaxHC )$**

**Where $|C1|+|C2|+|C3|=1$**

Route energy is taken as a factor keeping in view that MANETs have scarce energy resources. Using a route frequently while other routes are idle or under loaded may result in network instability. The aggregate interface queue length gives us the idea about how busy our route is. Its higher value depicts higher load on the route. Thus this parameter helps in determining the heavily loaded route. If each intermediate host has a large roaming area and the MANET has many nodes (and hops), then a feasible path with a low hop count is preferred and hence the metric hop count has been considered for route selection. Our protocol effectively combines all the three parameters with weighing factors C1, C2 and C3. The values of these factors can be

 

chosen as per the requirements, e.g. Energy being very critical for MANETs can have more weight than other factors. The adverse contribution to traffic distribution is built into negative coefficients. The path with the maximum weight value is selected as the primary routing path among all feasible paths.

## IV. RESULTS

In Fig.3 we can see the difference in security while using secured routing algorithms and without using any secured algorithms. This proves that security of network increases when we use the above routing algorithms to create a secured path and forward the data packets securely to the destination.

In Fig.4 it is clearly seen that power usage of node when we are not using any security algorithms is very huge because if any security mechanisms are not used the network will be vulnerable to many attacks which increases the power draining of nodes in the network. When we use the above given secured routing protocols it results in less power usage of nodes and transfers the data packets to the destination without coming in contact of any attacks.

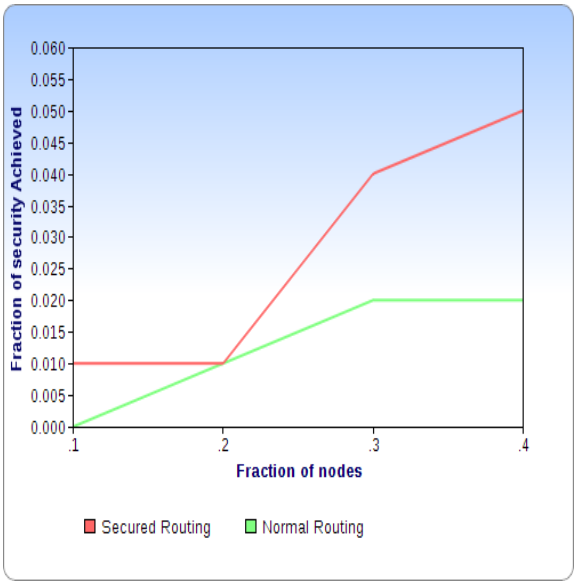


Fig. 3 Graph showing security in network using secured routing and normal routing

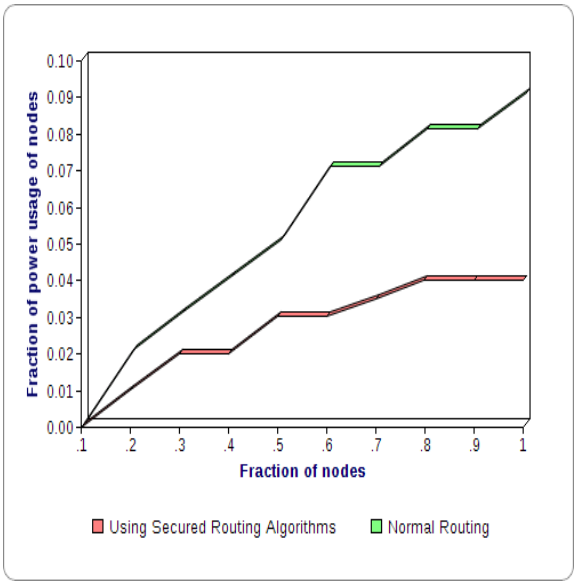


Fig. 4 Power usage of nodes using secured routing and normal routing

 

## V. CONCLUSION

In this paper we have shown that Ad hoc networks hold the key to the future of wireless communication, promising adaptive connectivity without the need for expensive infrastructure. In ad hoc networks, the lack of centralized control implies that the behaviour of individual users has a profound effect on network performance. In this paper we have investigated the performance of IEEE 802.11b ad hoc networks. Previous studies in this framework have pointed out that the behaviour of IEEE 802.11 ad hoc networks are complicated by the presence of hidden stations, exposed stations, attacks and so on. This paper has presented protocols for routing packets between wireless mobile hosts in an ad hoc network. Unlike routing protocols using distance vector or link state algorithms, our protocol uses dynamic source routing which adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently. In our proposed system we have shown how we generate a secure path to transfer the data by finding the topology of route and forward the data packets safely with the help of PLGP Protocol and AODV protocol. By this usage of protocols energy usage of nodes have also decreased.

## REFERENCES

[1] V. Rodoplu and T. H. Meng, "Minimum Energy Mobile Wireless Networks," IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8, August 1999, pp. 1333–1344.

[2] J.-H. Chang and L. Tassiulas, "Energy Conserving Routing in Wireless Ad Hoc Networks," Proc. of INFOCOM 2000, Tel Aviv, Israel, March 2000.

[3] A. Michail and A. Ephremides, "Energy Efficient Routing for Connection-Oriented Traffic in Ad Hoc Wireless Networks," Proc. Of the 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2000.

[4] V. Srinivasan, P. Nuggehalli, C-F. Chiasserini, and R. R. Rao, "Optimal Rate Allocation and Traffic Splits for Energy Efficient Routing in Ad Hoc Networks," Proc. of Infocom 2001, New York City, June 2001.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. of MobiCom 2000, Boston, August 2000.

[6] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J. P. Hubaux, and J.Y. Le Boudec, "Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes," IEEE Communications Magazine, Vol.39 No. 6, June 2001.

[7] L. Buttyan and J. P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," Technical Report No.DSC/2001/046, August 2001.

[8] L. Buttyan and J. P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs," Proc. of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Boston, MA, USA, August 2000.

[9] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao,"Energy Efficiency of Ad Hoc Wireless Networks with Selfish Users," European Wireless Conference 2002 (EW2002), Florence, Italy, February 2002.

[10] R. Perlman. Network Layer Protocols with Byzantine Robustness. PhD thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1988.

[11] R. Hauser, T. Przygienda, and G. Tsudik. Lowering security overhead in link state routing. Computer Networks, 1(8):885–894, April 1999.

[12] B. Kumar. Integration of security in network routing protocols. SIGSAC Reviews, 11(2):18–25, 1993.

[13] S. Murphy and J. J. Garcia-Luna-Aceves. An efficient routing algorithm for mobile wireless networks. MONET, 1(2):183–197, October 1996.

[14] K. E. Sirois and S. T. Kent. Securing the Nimrod routing architecture. In Proceedings of Symposium on Network and Distributed System Security, pages 74–84, Los Alamitos, CA, February 1997. The Internet Society, IEEE Computer Society Press.

[15] B. R. Smith, S. Murphy, and J. J. Garcia-Luna-aceves. Securing distance-vector routing protocols. In Proceedings of Symposium on Network and Distributed System Security, pages 85–92, Los Alamitos, CA, February 1997. The Internet Society, IEEE Computer Society Press.

[16] J. Jubin and J. Tornow, The DARPA packet radio network protocols, Proceedings of the IEEE 75, Special Issue on Packet Radio Networks (1987) 21–33.

[17] G. Lauer, Advanced protocols for the SURAN packet radio network, in: Proceedings of the SHAPE Packet Radio Symposium (1989).

[18] K. Chandran, S. Raghunathan, S. Venkatesan and R. Prakash, A feedback based scheme for improving TCP performance in ad-hoc wireless networks, in: Proceedings of International Conference on Distributed Computing Systems, Amsterdam (1998).

 

[19] R.C. Durst, G.J. Miller and E.J. Travis, TCP extensions for space communications, in: Proceedings of MOBICOM'96 (1996).
[20] S. Corson, S. Batsell and J. Macker, Architectural considerations for mobile mesh networking (Internet draft RFC, version 2), in: Mobile Ad-hoc Network (MANET) Working Group, IETF (1996).
[21] D.B. Johnson and D.A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks (Kluwer Academic, 1996).
[22] C.E. Perkins and E.M. Royer, Ad hoc on demand distance vector (AODV) routing (Internet-draft), in: Mobile Ad-hoc Network (MANET) Working Group, IETF (1998).
[23] V.D. Park and S. Corson, Temporally-ordered routing algorithm (TORA) version 1 functional specification (Internet-draft), in: Mobile Ad-hoc Network (MANET) Working Group, IETF (1998).
[24] Z.J. Haas and M.R. Pearlman, The zone routing protocol (ZRP) for ad hoc networks (Internet-draft), in: Mobile Ad-hoc Network (MANET) Working Group, IETF (1998).
[25] Charles E. Perkins and Pravin Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications, pages 234–244, August 1994.
[26] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensornetwork routing: A clean-slate approach, CoNEXT, 2006.
[27] N. Wang, Y. Huang and J. Chen, "A stable weight-based on- demand routing protocol for mobile ad hoc networks" Information Sciences 177(2007), pp. 5522-5537, 2007.

 