ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Protection based Routing Mechanism for Ad-hoc Network

Yogendra kumar Jain
Head of Department
Department of Computer Science & Engineering
Samrat Ashok Technological Institute
Vidisha, M.P., India
ykjain_p@yahoo.co.in

Geetika S. Pandey
Assistant professor
Department of Computer Science & Engineering
Samrat Ashok Technological Institute
Vidisha, M.P., India
geetika.silakari@gmail.com

Deshraj Ahirwar*
Department of Computer Science & Engineering
Samrat Ashok Technological Institute
Vidisha, M.P., India
deshrajahirwar.sati@gmail.com

Abstract: The Bluetooth Specification provides no specific support for positioning service. Bluetooth signal strength information to create a system for locating and tracking users inside buildings. The security of ad hoc networks is becoming an increasingly complex issue. Securing routing creates particular difficulties, since these networks have neither centrally administrated secure routers nor strict policies of use. The network topology is rapidly changing due to nodes in the networks being highly mobile, thus creating the presence or absence of links. Security requirements such as authentication, non-repudiation, data integrity and confidentiality, which would otherwise be provided by a central server, must be enabled and provided by all nodes. In this paper we propose enhance based direction routing protocol. The zone direction is reduced until the node can select the strongest and most stable link and so increase availability in the network. Each node in the network has a counter for the stability of link (SL) to its neighboring nodes, which indicates which nodes are active in the network, improving the performance of the network and increasing the likelihood of selecting the optimal path. We also propose a novel secure routing protocol to improve the security level in ad hoc networks, based on key management and a secure node-to-node path, which protects data to satisfy our security requirements.

Keywords: Ad-hoc Network, Routing Protocol, Security Mechanism

I. INTRODUCTION

Bluetooth offers a promising solution to indoor positioning. A separate working group called the Local Positioning Working Group has been created with an aim to develop a Bluetooth profile which describes the type and format of messages allowing Bluetooth devices to exchange position information and also the algorithm to compute the position. While it is going to take some time before the group comes up with a profile, the authors are currently involved in a project to investigate the Bluetooth performance for local positioning [1].

An ad hoc network works as an autonomous system of individual routers which are free to move randomly. Such a network is often characterized by rapidly changing and unpredictable wireless topology. Because the multiple nodes in such a system can enter and leave the system at any time, this system requires some sensing of the location and hence offers a very attractive environment to support context aware applications. The ad-hoc network provides limited automation needed in the position calculation and is an ideal and cheap alternative in the environment where the infrastructure is not developed yet. Bluetooth is one such emerging technology that provides ad-hoc networking [2].

The major challenges to *ad hoc* networks concern their design and operation, and result mainly from the lack of a centralized entity and infrastructural elements such as base stations, communication towers and access points. The possibility exists of fast node movement and all communications are conducted through a wireless medium.

These unique characteristics present nontrivial challenges for *ad hoc* networks [1] and [3].

As previously stated, many applications have recently become dependent on *ad hoc* wireless networks, and security is an extremely serious issue in any network. The dynamic nature of *ad hoc* wireless networks makes it extremely challenging to ensure secure transmission in these networks, which rely on the collaboration of all their nodes for their creation and efficient operation. While maintaining suitable routing information in a distributed way is a challenging issue in such networks, it is even more challenging to secure the protocols used for routing. At the network level, an *ad hoc* system fundamentally requires the routing protocols to be secured, as they enable a communication path to be established. On the other hand, the design of most such routing protocols gives no consideration to security, working instead with an implicit assumption of trust among the nodes. This provides the opportunity for malicious attackers, who may intend to bring down the network [2] and [4].

This paper proposes a new routing protocol: the Enhanced -direction Routing Protocol based on an on-demand routing scheme. We have added important features to overcome its disadvantages and improve its performance, providing the stability and availability required to guarantee the selection of the best path.

This paper also proposes a novel secure routing protocol for *ad hoc* networks: the Secure Enhanced Direction Routing Protocol. This is designed to improve the security level in *ad hoc* networks, based on key management and a

secure node-to-node path, which protects data to satisfy our security requirements: the detection of malicious nodes, authentication, authorization, confidentiality, availability, data integrity and a guarantee of secure correct route discovery.

II. BACKGROUND

The routing protocol has two main functions: the first is to find a feasible data packet path from a source node to a destination node; the second is to identify and exchange the routing information as a routing table, required for establishing the routing path, discovering path breaks, re-establishing or repairing broken paths and reducing bandwidth utilization. The nodes in an *ad hoc* network function as routers which discover and maintain routes to other nodes in the network. This absence of dedicated routers makes the provision of security a challenging task in *ad hoc* wireless networks, where the task of ensuring secure communication is also made difficult by factors including the mobility of nodes, limited processing power and limited availability of resources such as battery power and bandwidth [2].

A. Challenges in Routing:

The main challenges facing the routing protocol designed for *ad hoc* wireless networks are as follows:

a. Mobility of nodes:

The mobility associated with nodes, which is considered a primary characteristic of *ad hoc* networks, raises many issues such as packet collision, regular path breaks, stale routing information and difficulty in resource reservation. Their resolution requires a good routing protocol which is able to interpret them efficiently.

b. Other Resource Constraints:

Constraints on resources such as battery power and buffer storage can limit the capability of the routing protocol.

c. Error-Prone Channel State:

The bit error rate is very high in a wireless channel compared with its wired counterparts and the design of the routing protocol should take this into account. Taking into consideration the state of the wireless link, the signal to noise ratio and path loss for routing could improve the efficiency of the routing protocol.

d. Location-Dependent Contention:

As the number of nodes existing in a given geographical zone varies, so does the load on the wireless channel. Thus, if the number of nodes increases, this raises the contention for the channel. A good routing protocol can avoid such difficulties by means of inbuilt mechanisms for distributing the load uniformly across the network.

e. Bandwidth Constraint:

Since bandwidth for transmission is limited in *ad hoc* wireless networks, the bandwidth available per wireless link is based on the traffic each link carry and the number of nodes. Thus, a good routing protocol should keep bandwidth usage to a minimum [1] and [4] and [5].

B. Directional Angle Routing Protocol:

The core of the proposed schemes is the direction Routing Protocol, so called because it utilizes directional information on nodes in the network. Such information can be obtained from the node‘s own instruments and sensors, such as a compass, which delivers the -direction angle (HDA) of the mobile device relative to magnetic north. This protocol is used to reduce routing overhead and to increase the lifetime of links between nodes. It has been assumed that every node can exchange information frequently with its neighbours. Under HARP, every node classifies its neighbouring nodes into eight different zones according to their direction. In theory, the nodes are categorized within at least one of the eight zone ranges, regardless of their location. This protocol is based on an on-demand routing technique.

The RREQ packet is transmitted from a node to one of the neighbouring nodes that has an angular direction similar or near to the HDA of neighbouring nodes, where D is a value used for increasing the search around ND. When a source node S sends a request for a route to destination node D, it will look into its cache for D and if it is found, node S will start broadcasting the data packets to node D. If D is not found, a time Td will be initiated by source node S, where Td is the time required to find the destination. Then, node S starts searching in its cache for a neighbour that has a reference or near reference angle matching with or close to the HDA of S. This protocol reduces the overheads and minimizes bandwidth usage, since not all neighbouring nodes need to reply to a RREQ. Its main advantage is that it increases the lifetime of links between nodes. A disadvantage is that when the source node receives an error message, it will resend the request packet; the limited amount of sending avoids the formation of a loop without taking into account whether it knows the accurate path. Another drawback of HARP is the classification of different zones that are not suitable for the network if it is of high or low density. This protocol does not seem useful as an axis mapping technique, despite its use [5] and [6].

C. Hybrid Routing Protocols:

Hybrid routing protocols are designed to be both reactive and proactive in order to classify and offer different routing solutions. They increase the network‘s scalability, which allows nearby nodes to define a local zone, while determining routes to distant nodes using a reactive approach. In order to reduce route discovery overheads, neighbouring nodes work together by proactively maintaining routes to nearby nodes. Most proposed hybrid protocols are based on zones, which mean that the network is partitioned. Each given node partitions a zone of the network into two distinct regions. The routing zone for a particular node can be defined in terms of distance from that node or as lying inside a particular geographical region. This routing uses a proactive (table-driven) approach; a reactive routing approach uses nodes located in the area beyond the routing zone. The most typical hybrid types are the Zone Routing Protocol (ZRP) and the Core Extraction Distributed *Ad hoc* Routing (CEDAR) algorithm. The latter selects a minimum set of nodes as a core to perform quality of service route computations [7].

D. Secure Routing in Ad Hoc Wireless Networks:

The nodes in *ad hoc* wireless networks act both as regular terminals (source or destination) and as routers for other nodes in the network, unlike fixed wired networks such as the Internet, where dedicated routers are controlled by a service provider. This absence of dedicated routers makes the provision of security a challenging task in *ad hoc* wireless networks, where the task of ensuring secure communication is also made difficult by factors including the mobility of nodes, limited processing power and limited availability of resources such as battery power and bandwidth.

E. Security-aware Ad Hoc Routing Protocol:

The Security-aware *Ad hoc* Routing (SAR) protocol uses security as one of the key metrics to find paths, incorporating a structure for enforcing and measuring features of the security metric. This structure uses different levels of security for different applications that use the SAR protocol for routing. The communications between end nodes in *ad hoc* wireless networks are made through (possibly multiple) intermediate nodes, depending on the fact that the two end nodes trust the intermediate nodes. One of the tasks of SAR is to define the level of trust as a metric for routing. This means that every path for packets is associated with a security level, which is determined by a numerical calculation. A certain level of security is also associated with every intermediate node. When an intermediate node receives a packet it compares its level of security with that defined for the packet, and if the packet‘s security level is less than that of the node, then this node is considered to be a secure node and is permitted to view the packet. If it is greater, the packet is simply discarded. The SAR mechanism could easily be incorporated into traditional routing protocols for *ad hoc* networks. SAR permits the application to select the level of security it requires; however, the protocol requires different keys for different levels of security. The main disadvantage of this mechanism is that it tends to increase the number of keys required when the number of security levels used increases [3] and [8].

f. Authenticated Routing Protocol:

The Authenticated Routing *Ad hoc* Network (ARAN) protocol provides secure routing for *ad hoc* wireless networks by means of cryptographic certificates that successfully defeat all identified attacks in the network layer. It takes care of authentication, message integrity and non-repudiation, but expects a small amount of prior security coordination among nodes. In general, the main requirements it attempts to fulfill are first preventing things such as the spoofing of routing signals, the fabrication of routing packets, the shaping by adversaries of routing loops and the exposure by routing packets of the network topology; and secondly ensuring that such routing packets are not altered during transmission and that the shortest routing path is utilized. The major drawback of the protocol is that it needs a trusted certification server to issue the initial certificates. It offers security at two levels. The first, which is not fully secure, is an end-to-end authentication that is effective and requires low CPU power; however, it does not guarantee the shortest path usage. The second is stronger in security and guarantees to provide the shortest path, but requires more CPU power and resources. The ARAN protocol prevents compromised nodes from disrupting the network by providing route maintenance mechanisms and key revocation schemes [1] and [9].

g. Secure AODV:

The *Ad hoc* On-demand Distance Vector routing protocol provides security by securing the routing information. It uses schemes such as digital signatures, depending on source and end-to-end authentication. The protocol protects non-mutable data (not required or changed in the routing process) by use of public-key schemes. It secures the mutable data (necessary for the routing process), which in this case is the hop count information that uses hash chains. AODV uses a key management scheme and proposes a distributed CA to issue and validate the digital signature. The source performs the following three tasks:

a. It uses a public-key encryption scheme
b. It signs the data
c. It uses a hash function to encrypt the hop information.

On the path, every router will use a hash function to encrypt and update the hop information in order to secure it. When the destination receives the message, it uses the same hashing chain to verify the path and uses its keys to obtain the rest of the data and authenticate it. This scheme consumes less CPU power from the intermediate nodes, since they do not require access to the encrypted data. However, it still requires some authority structure to provide and manage the nodes with valid certificates [4] and [10].

h. Secure Efficient Ad hoc Distance Vector:

The Secure Efficient *Ad hoc* Distance vector (SEAD) routing protocol is a secure routing protocol for *ad hoc* wireless networks depending on the DSDV. This protocol protects against DoS attacks, reduces the overhead and speeds up the routing process, since it uses efficient one-way hash functions. It also assumes a limited network diameter in order to reduce the amount of information needed in the routing table and any exchange of information between nodes. As in secure AODV, it uses the incremental hash function of the route information to identify a correct path to the destination node. It also needs a similar security association between the source and destination nodes. SEAD avoids routing loops except the loop that includes more than one attacker. This protocol could be implemented easily with minor changes to the existing distance vector routing protocols. It is robust against multiple uncoordinated attacks. Nonetheless, SEAD is unable to defeat attacks where the attacker uses the same sequence number and metric which has been used by the latest update message and sends a new routing update [11] and [12].

III. PROPOSED ROUTING PROTOCOL MECHANISM

The mobility of mobile nodes and the stability of links to establish a robust and long-lived route between sources and destinations, in addition to reducing the flooding and overhead effects and minimizing the rate of breakage of links in the established paths. In the proposed approach, selecting nodes to forward packets between the source and the destination nodes is based on the Head Direction Angle (HAD) of these nodes and the stability of links between them. It should be borne in mind that the proposed approach

could be used as a stand-alone routing protocol under the limits and environmental conditions.

Now we presents the operation of the proposed enhancement of direction Angle Routing Protocol based on an on-demand routing scheme. We have added important features to overcome its disadvantages and improve its performance, providing the stability and availability required to guarantee the selection of the best path and to reduce the occurrence of broken links and dropped packets.

a. Each node in the network is able to classify its neighboring nodes according to their directions into four different zone-direction groups. The zone direction is reduced until the node can select the strongest link stability and so increase availability in the network.
b. Each node in the network has a counter for the stability of link (SL) to its neighboring nodes. The SL counter indicates which nodes are active in the network and this will improve the performance of the network and increase the likelihood of selecting the best or optimal path. The counter has an initial value of zero, which is increased by 1 after every successful sending or receiving and reduced by 1 after every failure in sending or receiving. The strongest stability of link is based on the greatest value in the counter.
c. This protocol is based on the time and acknowledgement message in order to guarantee the selection of the path and link stability.
d. Each node will send an acknowledgement message after receiving an RREQ and forwarding it, so the acknowledgement message should provide information on which nodes have problems or have been unable to forward the RREQ.
e. The source node should resend the RREQ whenever the time elapses before receiving the error message, in order to make use of the full lifetime of the links.

EHARP is an on-demand routing protocol which can be considered as comprising two parts: the mobility and classification of nodes and the discovery and maintenance of routes.

A. Enhance based Direction Routing Protocol Architecture:

Under enhance based direction routing protocol each mobile node in the network sends its mobility information to its neighboring nodes periodically and each classifies its neighboring nodes into four different zone-direction groups (Z1, Z2, Z3, Z4). As can be seen in Figure 1, according to their directions, each mobile node in the *ad hoc* wireless network divides the directions into different sectors. The directions between 0° and 90° comprise zone-direction 1 (Z1); those between 90° and 180° comprise zone-direction 2 (Z2) and so on.

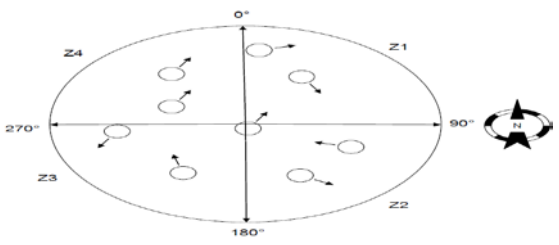

Figure1: The four basic direction ranges and neighbours classified in these ranges

After the source node *S* has classified its cache table, as shown in Figure 1, and wants to send a request packet to its neighbour, *S* then selects that neighbour. This selection depends on two factors; the first being that it has an angular direction of one of the four axis angular values (0°, 90°, 180°, 270°) $\pm\delta$, where δ is an angular value that represents the range of angles that are considered near to the axis. The second factor is the value of the link stability of its neighbours. The neighbouring nodes of a mobile node are categorized within at least one of the four zone ranges, regardless of their actual positions relative to the mobile node itself.

a. Route Discovery:

The route discovery process initiated at the source node and the intermediate nodes (all nodes except the source and destination). It also covers the route maintenance and local repair mechanisms that are executed when a link is broken.

B. Route Discovery at the Source Node:

At the source node, when a source *S* requests route to a destination *D*, it will look in its cache for the destination node *D* and if it is found as a neighbour, *S* will start forwarding the data packets to *D*. If *D* is not found in the source cache, *S* will set a determined time *Td* within which the destination node must be found. *S* then searches its cache for a neighbour that has a reference or near reference angle, matching with or close to the direction angle of *S*, and the greatest value of SL, in order to extend the lifetime of the route.

Therefore, for the best matching and finding a neighbour with nearly similar direction to the node itself and the greatest value of SL, this protocol performs well in a network where nodes form groups and where each group moves together in one direction, such as in military vehicles on a road. This protocol performs better than other existing routing protocols that use the technique of flooding the route request across the network to reach the target destination, by controlling the flooding by those nodes that let the link last longer. Here, after searching for a neighbour in the cache memory of *S*, there are two possibilities:

i. If *S* does not find a neighbour in its cache by axis mappingor the only neighbour has a negative SL value, it will apply an increment of $\pm\delta$ around the angle of *S*, to widen the search for another neighbour in a new direction. If no neighbour is found in the time *Td*, a route request will be triggered again (*S* will repeat the RREQ for a limited number of times, to avoid the search-to-infinity, while excluding neighbours that have been selected in previous tries at finding D.
ii. If *S* finds a neighbour in its cache, then where more than one neighbour is found, the greatest value of SL will be selected. *S* will initiate an RRL and add its information record to that list. Each record has the following fields: node IP, node angle, zone range area, *Td*, SL. The route request packet will then be broadcast along a selected angle of a neighbouring node. The steps followed at a source that has data packets to send to node *D*. The *Max RREQ Count* is the maximum number of RREQs allowed to be sent to search for a particular destination. *S_Dir*is the direction angle of *S* and *S_Zone*is the zone of *S* (Zone 1 between 0° and 90°, Zone 2 between 90° and 180°, and so on). *Nb_Dir*is the direction angle of the neighbour*Nb*,

*Nb_SL*is the stability of the corresponding link and *Max acceptable HDA* is the maximum accepted angle around its HDA axis that the node uses to search for a neighbour.

The source node will again trigger a route request:

a) If it does not find a neighbour in the time *Td* (*S* will repeat the RREQ a limited number of times, to avoid the risk of search-to-infinity). Each time, it will apply an increment of $\pm\delta$ around the angle of *S*.
b) If it does not receive a route reply from *D* in *Td*.
c) If it receives an RREP from *D* before *Td* has elapsed.

a. Route Discovery at Intermediate/ Relay Nodes:

At intermediate nodes, all the nodes that receive the route request message update their route cache entries by updating the information of the neighbouring node from which the message was received; only the intermediate node to which the RREQ message is addressed will accept it, while other nodes will silently drop it. The intermediate node to which the message is addressed will search in its cache of neighbours for *D*, then:

i. If the intermediate node is found, *D* in the cache table will be updated in the RRL by adding the record containing the information about the node itself, then it will broadcast a reply message along the nodes that have records in their RRLs backtracked to the initiating source node.
ii. If the intermediate node does not find *D* in the cache table, axis mapping will apply, increasing the angle of *S* by $\pm\delta$ to extend the search for another neighbour with the greatest value of SL in a new direction. Before forwarding the route request message, the intermediate node will add a record to the RRL containing information about the node itself. It will then set up a determined time *Tn*within which a neighbour must be discovered. After the intermediate node forwards the RREQ, an acknowledgement message will be sent to *S*.
iii. Each intermediate node identified again triggers an RREQ, which will be checked in the cache memory to see whether it has received an acknowledgement message from its nearest neighbour. This will be propagated to the same neighbour. If it has not received an acknowledgement message from its nearest neighbour, then an increment of $\pm\delta$ will be applied around the angle of S to extend the search for another neighbour in a new direction. Figure 5.3 shows the actions performed at the intermediate node.

b. Route Reply:

A route reply message is triggered in two cases:

i. When it receives the route request packet, *D* will piggyback the RRL that is included in the route request in the reply message, which it will send along the reverse path determined by the nodes recorded in the RRL.
ii. When the intermediate node has received the route request message and has information about the destination stored in its cache (a valid path to *D*), the intermediate node will update the RRL by adding its information and piggyback the RRL in the reply message, then send it along the reverse path determined by the nodes recorded in the RRL.

c. Secure Enhanced Direction Routing Protocol:

Our main focuses are to introduce Secure Enhanced Direction Routing Protocol to protect data transmission and to construct a secure routing protocol. The network consists of a group of mutually trusting nodes. There are two types of node, which are:

i. User Node (UN): Normal ground nodes, typically soldiers.
ii. Network Backbone Node (NBBN): Usually units or master nodes located within the network, for example tanks. NBBNs can establish direct wireless links for communication amid themselves Secure Enhanced Direction Routing Protocol works as a group and has three stages, examined in turn in the remainder of this section:
iii. Distribution of keys and certificate stage.
iv. Secure path stage.
v. Secure routing protocol stage.

d. Distribution of Keys and Certificate Stage:

Our scheme adopts the NBBN approach because of its superiority in distributing keys and achieving integrity and non-repudiation. The system uses private and public keys. The private key is used to sign the certificate and the public key of all the nodes, while the public key is used to renew certificates that are issued by another NBBN. All nodes must have a copy of the NBBN‘s own public key to verify signatures. The public keys and the corresponding private keys of all nodes are created by the NBBNs, which also issue the public-key certificates of all nodes. Each node has its own public/private key pair. Public keys can be distributed to another node in the secure path stage, while private keys should be kept confidential to individual nodes.

The NBBN signs the public key certificate for all nodes, so that these signings take place offline before the nodes can enter the network. Each node in our approach receives exactly one certificate after securely authenticating its identity to the NBBN. Each node will hold its digital certificate in the Node Databases (NDB). The main structure of node digital certificates, it contains the identifier of the node, its public key, the name of the NBBN issuing this certificate, the certificate issue and expiry dates, and the public key of the NBBN. Finally, the contents of the certificate will be attached to the digital signature of the NBBN. All nodes in a network should maintain fresh certificates with the NBBN. At the secure path stage, nodes use their certificates to authenticate themselves to other nodes in the network.

e. Secure (node-to-node) Path Stage:

Our approach is to use a public-key algorithm to establish secure paths between nodes. The Secure Path Stage (SPS) is based on the requirement for all nodes to have a secure path with other nodes before sending any route request packet. Any node receiving an RREQ from the source node or another node without a secure path should discard the request. In our approach, each node is given the system public key in order for any node to be able to send a Secure Path Request (SPR) to another node the first time the certified public keys are exchanged. The authenticity of the certificate can be confirmed as the nodes have the system public key. The first objective of the SPS is the exchange of the certified public keys and their confirmation, while its second objective is to ensure the identity of the sender

before acceptance of the RREQ. The SPS considers secure authentication node by node.

f. Secure Routing Protocol Stage:

At this stage, our Secure Enhanced Direction Routing Protocol approach uses a hybrid of security mechanisms so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash function, digital signature, time synchronization and route discovery request.

g. Hash Function-

The hash function is used to encrypt and update the data necessary for the routing process in order to secure the mutable data, which in this case is the head direction and time to find a destination, whose information uses hash chains. Secure Enhanced Direction Routing Protocol uses hash chains in order to secure the mutable data of the head direction and Td, the maximum time to find a destination node, for any node in the network, including an intermediate node and the destination node, which when it receives the message can verify that the mutable data has not been decremented by any attacker. Secure Enhanced Direction Routing Protocol forms a hash chain by applying it one way. A hash function is the operation whereby a node creates an RREQ or RREP and a hash function repeatedly to begin. The setting of the hash function is as follows:

i. Assign a random number to the Hash field as the beginning value, so that Hash = beginning.
ii. Set the MaxHashCount field to the time to find destination value from the IP header, i.e. MaxHashCount = *Td*.
iii. The Hash_Function field is set to indicate which hash function is employed: Hash_Function = h.
iv. Calculate Top_Hash by hashing beginning value as hash_Count.

- *Top_Hash= h* MaxHashCount – *h hash_Count*
- *Hash Count = time to find neighbour*
- Where *h* is a hash function and *h j (y)* is the result of applying the function *h* to *y j* times.

When a node is retransmitted an RREQ or an RREP packet is used to verify the hash count. The node performs the following operations: 1. It applies the hash function indicated by the *Hash_Function*field MaxHashCount minus Hash Count to the beginning value in the Hash field and verifies that the value is equal to the value contained in the Top_Hash field. *Top_Hash=(h* MaxHashCount – *h Hash_Count).* 2. Before rebroadcasting an RREQ or forwarding a RREP, a node uses the hash function from the Hash value for the new node: *Hash = h (Hash).*

h. Digital Signature-

A digital signature is used to protect the non-mutable data, which is data not required or changed in the routing process. Digital signatures provide authentication and data integrity and ensure non-repudiation. Proposed Secure Enhanced Direction Routing Protocol has two digital signatures. The first is the source signature used to protect the integrity of the non-mutable data in RREQ and RREP messages, which means that the source signs everything.

The second is the node-by-node signature, based on who obtained a secure path, and every intermediate node afterwards verifies the hash function, updates information and provides a signature for the updating. When a node receives an RREQ, it first verifies the signature of the sender and of the secure path before creating or updating a route to that neighbour. Only if the signature is verified will it update a route and set *Td* to find the neighbour. After it is updated, it will sign all new updating and fields node by node from the RREQ. In the event of a failure, it will discard the RREQ. The destination node, when it receives an RREQ, first verifies the signature of the source and the signature of the intermediate node that has a secure path by field signature node-to-node. In the event of a failure, the RREQ will be discarded.

i. Time Synchronization:

A timestamp is used to protect the route path from specific attacks. The Enhanced Direction Routing Protocolprotocol is based on the time to find the destination and neighbouring nodes. When a node has a request packet, it calculates the time to find a neighbour and destination, and after creating the packet uses the timestamp; then the node that has received the packet must verify it from the timestamp.

We presented a secure routing protocol based on key management, a secure path and protecting data to satisfy our security requirements. After understanding security requirements and identifying the types of attack the network might face, we proposed the security mechanism most able to satisfy these security requirements, having the following elements:

i. asymmetric encryption (used to protect non-mutable data)
ii. hash function (used to protect mutable data)
iii. Time synchronization.

All these mechanisms when applied to routing protocols should prevent external attacks, including black holes and routing holes, while providing viability, confidentiality and authentication. Time synchronization is used to provide the protocol with the ability to find the route and to ensure that the selected route is the correct path. The digital signature mechanism, when applied to routing protocols, should prevent internal attacks, including impersonation, and should provide non-reputation and integrity.

IV. RESULT ANALYSIS

Our experimental results of the proposed Enhanced Direction Routing Protocol and Secure Enhanced Direction Routing Protocol against the routing protocols. The results show that Enhanced Direction Routing Protocol clearly offers a significant reduction in the cost of route discovery packets (overhead) in comparison with routing protocol and that this scheme is less affected by mobility, speed and number of nodes than routing in terms of the efficiency of data packet delivery It was noticed, however, that the increased average end-to-end delay under Enhanced Direction Routing Protocol put it at a disadvantage compared to routing protocol. In spite of this limitation, in many applications, finding the path that lasts longest with reduced overhead and collisions and with an acceptable level of delay is crucially important; furthermore, this acceptable delay is application dependant. In terms of route discovery, at elapsed times, Enhanced Direction Routing Protocol was found to perform better than Direction Routing Protocol, while at longer elapsed time, Enhanced Direction

Routing Protocol performed better than normal routing. Enhanced Direction Routing Protocol was found to perform better in route discovery against speed than either Direction Routing Protocol.

The second set of quantitative analyses compared the performance of the proposed security protocol, Secure Enhanced Direction Routing Protocol, with Enhanced Direction Routing Protocol, using the same evaluation metrics. The algorithm performed well in scenarios where mobility, speed and network size were varied. The simulation results show that Secure Enhanced Direction Routing Protocol functions very similarly to the Enhanced Direction Routing Protocol and better than Direction Routing Protocol.

V. CONCLUSION

Designing communication protocols and applications for such networks is very challenging due to the absence of fixed infrastructure, the inevitable mobility and constrained bandwidth. It is crucial in *ad hoc* wireless networks to deliver data packets effectively, minimize connection breakdown and control packet overhead, while ensuring that a route remains connected for the longest possible period. The mobility of the nodes of these networks presents the most difficult challenge to routing protocol designers, because it causes frequent topology changes and route invalidation, which increase the signaling overhead required to establish routes, thus affecting the performance of the routing protocols. The main contributions of this work to the existing literature on the subject are the definition of the architecture for the Enhanced Direction Routing Protocol and the new secure routing protocol (Secure Enhanced Direction Routing Protocol) for *ad hoc* wireless networks. Both Enhanced Direction Routing Protocol and Secure Enhanced Direction Routing Protocol are unique in the respect that no comparable proposals have been made. In addition, the secure environment approach is applied to the problem of regulating access to a hostile environment in an *ad hoc* wireless network. The *ad hoc* environment assumption and the way it is used in defining these protocols is of itself a novelty.

VI. REFERENCES

[1]. Lavanya, C. Kumar and A. Rex Macedo Arokiaraj, "Secured Backup Routing Protocol for AD HOC Networks', IEEE 2010 International Conference on Signal Acquisition and Processing.

[2]. YongQing Ni, DaeHunNyang and Xu Wang, "A-Kad: an anonymous P2P protocol based on Kad network", IEEE 2009.

[3]. N.Bhalaji, Dr.A.Shanmugam, "ASSOCIATION BETWEEN NODES TO COMBAT BLACKHOLE ATTACK IN DSR BASED MANET", IEEE 2009.

[4]. SohailJabbar, Abid Ali Minhas, Raja AdeelAkhtar, Muhammad Zubair Aziz, "REAR: Real-time Energy Aware Routing for Wireless Adhoc Micro Sensors Network", 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[5]. D.Suganya Devi and Dr.G.Padmavathi, "Performance Efficient EOMCT Algorithm for Secure Multicast Key Distribution for MobileAdhoc Networks", IEEE 2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[6]. JianRen and Yun Li and Tongtong Li, "Providing Source Privacy in Mobile Ad Hoc Networks", IEEE 2009.

[7]. Matthew Tan Creti, Matthew Beaman, SaurabhBagchi, Zhiyuan Li, and Yung-Hsiang Lu, Multigrade Security Monitoring for Ad-Hoc Wireless Networks", IEEE 2009.

[8]. R.PushpaLakshmi and Dr.A.Vincent Antony Kumar, "Security aware Minimized Dominating Set based Routing in MANET", IEEE 2010 Second International conference on Computing, Communication and Networking Technologies.

[9]. Singh S., Raghavendra C.S., "Power efficient MAC protocol for multihop radio networks", Personal, Indoor and Mobile Radio Communications, 1998. The Ninth IEEE International Symposium on, Volume: 1 , 8-11 Sept. 1998, pp:153 – 157.

[10]. Perkins C.E., Royer E.M., "Ad-hoc on-demand distance vector routing Mobile Computing Systems and Applications", Proceedings. WMCSA'99. Second IEEE Workshop on, 25-26 Feb. 1999, pp: 90 – 100.

[11]. Gregory Lamm, GerlandoFalauto, Jorge Estrada, and Jag Gadiyaram. Bluetooth Wireless Networks Security Features.Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, June, 2001.

[12]. N. Asokan and P. Ginzboorg. Key Agreement in Ad-hoc Networks. Computer Communications 23(17), Nov. 1 2000.