MHRP: A SECURE MULTI-PATH HYBRID ROUTING PROTOCOL FOR WIRELESS MESH NETWORK

Muhammad Shoaib Siddiqui, Syed Obaid Amin, Jin Ho Kim, Choong Seon Hong
Kyung Hee University
Korea.

ABSTRACT

Wireless Mesh Network is a new and promising paradigm in wireless networks that allows network deployment at a much lower cost. Routing is the main research issue in the development of Wireless Mesh Networks. Many of the routing approaches have been borrowed from Wireless Mobile Ad hoc Network to achieve routing solutions in Wireless Mesh Networks but these approaches are not ideal or optimal. These routing protocols can be distinguished as proactive and reactive routing protocols. As a Wireless Mesh Network is itself a hybrid network solution among ad hoc and static networks, a hybrid routing approach is required. In this paper, we provide the secure multi-path version of this hybrid routing protocol, which enhances the reliability in the network, provide secure routing and has efficient techniques of finding alternate routes when a route is lost. We provide comparisons of this routing protocol with other routing protocols that are available for Wireless Mesh Networks[1].

I. INTRODCUTION

Wireless Mesh Network (WMN) [1] is an emerging new technology which is being adopted as the wireless internetworking solution for the near future. Characteristics of WMN such as rapid deployment and self configuration make WMN suitable for transient on-demand network deployment scenarios such as disaster recovery, hard-to-wire buildings, conventional networks and friendly terrains. WMN is also an attractive technology for long-lived infrastructure networks such as wireless municipal area network in dense metropolis, heterogeneous networks and for providing low-cost backhaul to cellular base station in remote rural areas and to sensor networks.

The form of mesh networks that are of most commercial interest are often called hybrid mesh networks [2], shown in Fig. 1. In Hybrid mesh networks, the end users such as PDAs and laptops make up mesh client networks while mesh router nodes are part of the network infrastructure [2]. Here, the network consists of two types of links: short range wireless links (shown in Fig. 1 as dotted lines) among client mesh nodes and mesh relay links (shown in Fig. 1 as dashed lines) between router nodes to form the packet transport backbone.

Since the nodes in ad hoc components can be highly mobile, the topology changes frequently within the ad hoc region and the nodes are dynamically connected in an arbitrary manner. Moreover these wireless clients have low transmission power, limited computation power and limited radio ranges. The small transmission range limits the number of neighboring nodes, which in turn increases the frequency of topology change, owning to node mobility. All these factors add up to make routing difficult.

For a specific solution of this routing problem, not much research has been done; instead routing protocols developed for ad hoc networks are being used in WMNs. These protocols can be classified as reactive and proactive protocols; but due to their technical constraints [2], they are not able to provide an optimal solution to this critical issue of routing in Wireless Mesh Networks. A hybrid protocols can be used to find a balance between the proactive and reactive protocols. The basic idea behind hybrid routing protocols is to use proactive routing

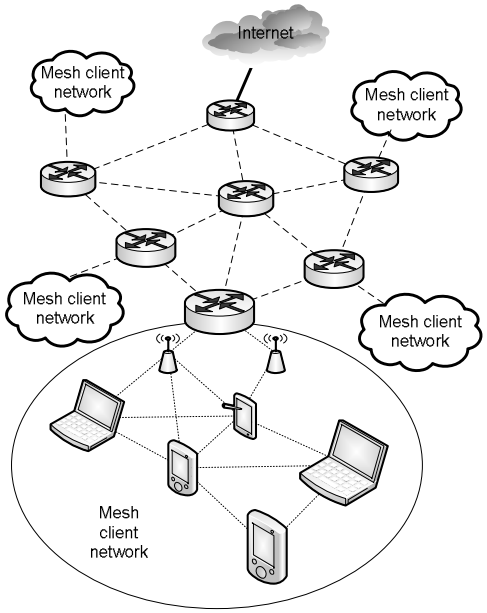

Figure 1. A hybrid wireless mesh network.

1-4244-1513-06/07/$25.00 ©2007 IEEE
* "This work was supported by ITRC and MIC."

mechanisms in some areas of the network at certain times and reactive routing for the rest of the network.

For providing secure communication in WMNs; there are two ways: (1) Using the multiple paths [3] available in between the two nodes. (2) Using the cryptographic methods to secure the communication in between two nodes. In first approach all the multiple paths between two nodes need to be node-disjoint (a node cannot participate in more than one path between two end nodes). If there are k multiple paths available then the adversary requires compromising at least k nodes – and more particularly at least one node in each path – in order to control the communication. This approach is cost effective as it does not include any computation or transmission overhead and hardly inject delay in the network. But it does not ensure a certain level of security as there are not always multiple paths between two end nodes.

The second approach may provide optimal security but with the price of too much computation and transmission cost as well as time delay. Multi-path routing protocols need to be properly enhanced with cryptographic means which will guarantee the integrity of a routing path and the authenticity of the participating nodes. However, the cryptographic protection such as public key cryptography, increase the control overhead and produce significant delay thus diminishing the efficiency of the secure multi-path routing protocol.

In this paper, we address the routing concern of WMNs by proposing a hybrid multi-path routing protocol .We also provide a simple mutual authentication mechanism which significantly reduces the control overhead of secure multi-path routing protocols. In section 2, we provide introduction to related approaches in the secure multi-path routing field. In section 3, we provide the architectural introduction to our hybrid multi-path routing scheme. In section 4, we discuss the mechanism that makes our multi-path routing scheme secure and reduces complexity and security control overhead. In section 5, we present the simulations and analytical comparison of our proposal with related work. In section 6, we conclude our proposal and discuss the future work.

II. RELATED WORKS

In WMNs, nodes have relatively fixed positions and communicate to the Internet through one or more gateways. While traditional ad-hoc routing algorithms, such as DSR [6] and AODV [5] can be used in WMNs, their performance is typically less than ideal [2]. The problem is that such algorithms make assumptions (such as very high node mobility and no Infrastructure) which are no longer true in WMNs [2] and those assumptions can have a significant impact on the routing performance in mesh environments. A number of routing protocols [2] have been suggested for WMNs. These protocols can be classified as proactive and reactive protocols.

Proactive protocols are table-driven and actively determine the layout of the network. Through a regular exchange of network topology packets between the nodes of the network, a complete picture of the network is maintained at every single node [6]. Hence, there is minimal delay in determining route to the destination. This is especially important for time-critical traffic. Examples of proactive protocols include: OLSR [6], DSDV [7] etc.

Reactive protocols only find a route to the destination node when there is a need to send data [8]. The source node will start by transmitting route requests throughout the network. The sender will then wait for the destination node or an intermediate node (that has a route to the destination) to respond with a list of intermediate nodes between the source and destination. Examples of reactive protocols include: AODV [5], DSR [6], TORA [7] etc.

Multi-path routing protocols [3] were initially designed for providing reliability [9] and QoS in the ad hoc networks. But their nature of attack resilience was quickly identified as a significant security feature. Indeed, with single path routing protocols, it is easy for an adversary to launch routing attacks. A compromised node controlled by the adversary may participate in route discovery between two end nodes without being noticed. Hence, the adversary can control the routing mechanism and disrupt the services at any instance.

Secure multi-path routing protocols are more resilient to routing attacks than typical routing protocols [10]. Although a lot of work is being done in the field of routing protocols in WMNs but little effort is put up for a secure routing protocol. Many solutions proposed for Mobile Ad hoc NETworks (MANETs) are adopted as a solution for WMNs. As WMNs have somewhat similarity with MANETs, these protocols work fine in WMNs but do not utilize the characteristics of WMNs to their benefits. However, there are some protocols which are good enough to be implemented in WMNs and provide a secure multi-path routing solution such as SRP [11] and SecMR [12].

A secure multi-path routing protocol called Secure Routing Protocol (SRP) [11] by Papadimitratos and Haas was initially developed considering the general security of ad hoc networks. Another approach was provided by Burmester and Van Le [4], which is based on the Ford-Fulkerson maximum flow algorithm. Kotzanikolaou et al

presented Secure Multi-path Routing (SecMR) [12] protocol to reduce the cost of node authentication. SecMR works in two phases: mutual authentication and route discovery phase. At the end of route discovery, the end nodes use a symmetric key in order to verify the integrity of the discovered paths. SecMR provide multiple paths along with routing security and is better than the other two protocols. However, due to the use of digital signature in periodic mutual authentication phase, the computation cost and control overhead incurred render this scheme inefficient.

III. HYBRID MULTI-PATH ROUTING IN WMN

A. Motivation

Wireless mesh networks were developed for reliable data communication and load balancing. Multiple path communication is the basic need behind these two attributes. If these attributes of WMNs are not utilized properly; one cannot achieve the best out of this network paradigm. Moreover, multi-path routing assists in achieving security in routing protocols. Schemes discussed in section 2 are not designed specifically for WMNs. Therefore, most of the proposed schemes are not able to utilize the best features of WMNs. These limitations urge a need of a routing protocol specifically tailored for WMNs. In the light of these works, a solution for secure multi-path routing is required which proficiently utilize the characteristics of wireless mesh networks as well as use the best algorithms of network security.

Both proactive and reactive protocols have specific advantages and disadvantages that make them suitable for certain types of scenarios. Since proactive routing maintains information that is immediately available, the delay before sending a packet is minimal. On the contrary, reactive protocols must first determine the route, which may result in considerable delay if the information is not available in the caches.

Moreover, the reactive route search procedure may involve significant control traffic due to global flooding. This, together with the long setup delay, may make pure reactive routing less suitable for real-time traffic. Purely proactive schemes use a large portion of the bandwidth to keep routing information up-to-date. Due to fast node mobility, the route updates may be more frequent than the route requests and most of the routing information is never used. Some part of the scarce bandwidth is thus wasted [6].

As we look at the architecture of Wireless Mesh Networks, we can conclude that both these types of protocol face problems in providing a solution [6]. A better solution would be to use different routing protocols for the different parts of the hybrid WMN. For ad hoc components we can have a reactive protocol to counter the dynamic changes in topology and the mobility of the nodes. A proactive protocol would be better suited for the static router infrastructure so as to provide immediate availability of routes in the backbone WMN. On the basis of this concept we propose a hybrid protocol which promises to provide a better solution to the routing problem.

B. Assumptions

Hybrid wireless mesh network has more commercial interest than the other two types of wireless mesh networks because it is the most applicable case [2]. Our proposed mechanism is for hybrid wireless mesh; a network in which there is a router infrastructure providing a routing backbone and many client mesh networks called ad hoc regions, which consists of mobile client devices. These client nodes have limited computational, transmission and electrical power.

A router from the mesh infrastructure manages each ad hoc region such as providing addresses, assisting routing and providing security. We also assume that there is a Certificate Authority (CA) [13] in the wireless mesh network, which is a trusted third party that can authenticate the digital certificates of the nodes. Every node is provided with a pair of public and private key during the deployment phase.

C. Architecture

Our proposed Routing protocol consists of four components, as shown in Fig. 2. These components are:

- Intra Region Routing Protocol – IRRP
- Router Infrastructure Routing Protocol – RIRP
- Region Gateway Routing Protocol – RGP
- Route Maintenance Protocol

RIRP is a family of proactive protocols used in router Infrastructure WMN. As the routers in the infrastructure mesh are relatively static with high bandwidth communication links, we keep the route up to date. Small 'Hello' packets are sent by each router to its neighbor routers at a constant interval to keep the routing table fresh and accurate. When a new router comes into the backbone mesh it broadcasts 'hello' packet and its routes are updated by the other routers' update messages. These updated route tables do a very good job in reducing the delay in route determination. RIRP uses Ford-Fulkerson maximum flow algorithm. Each node sends its neighborhood information and broadcast the hello packet. When the other nodes receive these messages, it performs the maximum flow algorithm and calculates all the possible node-disjoint

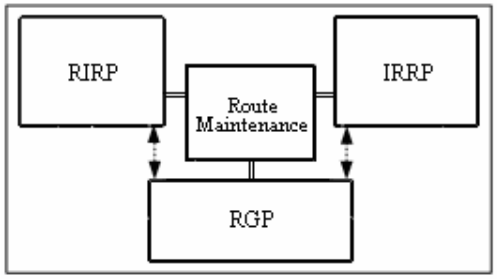

Figure 2. A conceptual architecture of the Proposed Protocol.

paths. Hence, this protocol provides complete set of paths. Each node maintains all possible paths to the other nodes and uses the best path for communication. Whenever a link is lost an alternative route is selected from the routing table.

In an ad hoc region or client mesh the routes are maintained through a protocol component specified as Intra-Region Routing Protocol (IRRP). IRRP is a family of reactive routing protocols that offer enhanced route discovery and route maintenance services based on local connectivity within the ad hoc region. The client nodes have greater mobility and this causes frequent changes in topology and consequently there is a change in the routing information, therefore, the routes need to be updated at a higher rate. Hence a reactive routing protocol is required that only finds the route at the time of transmission. IRRP is a multi-path derivative of AODV [5] routing protocol, which uses forward selection to find alternate paths when a link is down. In IRRP, intermediate nodes create multiple reverse paths towards the source while forwarding the route request. When the route reply is sent back to the source, multiple disjoint routes are created from the destination to the source node. Each intermediate node also preserves the alternative link information to the destination node for future use. When a link is lost, intermediate nodes can work up a new route, hence, decreasing the route latency in finding alternate routes.

The Region Gateway Protocol (RGP) is used whenever the routes between two ad hoc regions are required. It gets routes' information from the RIRP and IRRP and creates complete routes from source to destination and provides them to the source node. This is shown in Fig. 3. There is one RGP component for the entire network, one RIRP for the router backbone and several IRRP components for separate ad hoc regions. When a node requires a route it first sends the route request (shown in Fig. 3 as message 1) to RGP running on the wireless router in its region. The router gets the route information from RIRP (message 2 & 3) and IRRP (message 4 & 5) of destination node's ad hoc region and finally constructs the available multiple routes and sends them to the source node (shown as message 6 in

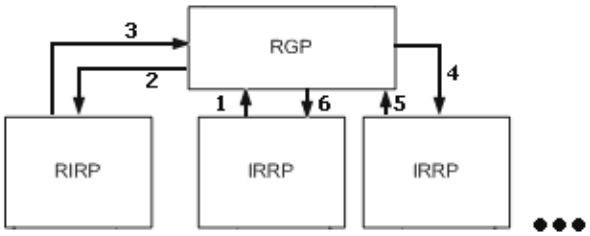

Figure 3. Route Request/ Reply; flow of route messages within the routing components.

Fig. 3). Routing tables of all the participating nodes are updated as messages pass to and from the client nodes and routers. Route maintenance protocol maintains the routing table and provides alternate routes whenever required.

Whenever a new mesh router node is added to the system or in case of link failure; RIRP needs to know about the event. For this, RIRP makes use of either Neighbor Discovery Protocol (NDP) provided by Media Access Control (MAC) layer or provides this functionality itself. Each node sends 'Hello' packets to other nodes in the neighborhood at constant interval. If timeout occurs and the 'hello' packet is not received, then there is a problem within the link. Similarly, when a new node enters it can advertise itself by broadcasting a 'hello' packet.

D. Routing

Whenever a node has to send some data to another node, it checks if it has the route to destination; if not it starts the route discovery phase. The route discovery mechanism has three stages: route request, route formation and route reply. In route request, a route query is sent to the neighboring nodes using IRRP; if the neighboring nodes do not have the route to the destination they forward the request to other nodes. If no node has the route to the destination the request is sent to RGP running on the router connected to the ad hoc component. Here RGP tries to find whether the router connects to the destination ad hoc component using the RIRP. When the route to the router node is found RGP uses IRRP in the ad hoc region in which the destination node is, to find the route to the destination node. After the routes to the destination are found, the whole routes from source to destination are formed by the RGP. This phase is called the route formation phase. When the whole routes are formed, a route reply containing the whole routes is sent back to the source node which constitutes the last phase of route discovery.

If the receiving node exists in the same ad hoc region as the sending node; only reactive routing is used. The IRRP discovers the possible routes and the data are sent through the discovered routes. If the receiving node and the sending nodes are not in the same region then route

discovery is done by using both reactive and proactive routing protocols. The route request phase is then further divided into two phases: the proactive phase and a reactive phase. The router node connected to the ad hoc region of the sender node is responsible for the proactive phase and the router node connected to the ad hoc region of the destination node is responsible for the reactive phase.

First the router node of the sender node discovers the route to the ad hoc region of the destination node with the help of RIRP. Then the router node at the receivers' ad hoc region performs the reactive route determination using IRRP to find the route to the destination node. Region Gateway Protocol is responsible for creating a whole route from the two routes discovered through the RIRP and IRRP and send it to the source node.

IV. SECURITY MECHANISM

After a new node comes into an ad hoc region, the public key of the router node assures the authenticity and integrity of the following messages as all those messages are encrypted by the private key of the router node.

The client node and the router node encrypt the messages by their private keys before sending them to each other. This process authenticates both the nodes. For the authenticity of each other, the router node or the client node can contact the CA to verify the digital signature of each other. During this time of mutual authentication both node share a secret key using authenticated Diffie-Hellman [14] algorithm so that in the future they are not required to use public key cryptography. In the same way all the nodes within an ad hoc region has a secret key shared by the manger router of that region. The algorithm is stated in the next sub-section.

The second phase is the key deployment phase among the client nodes. The router node distributes the keys calculated through a hash chain to all the client nodes for intercommunication. These are the secret keys which would be used by the client nodes to provide secure multi-path routing in the wireless mesh network.

A. Algorithm

The algorithm for authenticated Diffie-Hellman [14] for sharing a secret key between the router node R and the client node E is as follows:

Step 1. ***R*** *&* ***E*** *each possess a public/private key pair and a certificate for the public key.*
Step 2. ***R*** *&* ***E*** *agree to use a prime number p and g.*
Step 3. ***E*** *chooses a secret integer a, then sends* ***R*** *(g^a mod p) together with its signature and public key certificate.*
Step 4. ***R*** *chooses a secret integer b, then sends* ***E*** *(g^b mod p) together with its signature and public key certificate.*
Step 5. ***E*** *computes $K = (g^b \bmod p)^a \bmod p$*
Step 6. ***R*** *computes $K = (g^a \bmod p)^b \bmod p$*
Step 7. Shared Secret key is K; ***E****'s private key is 'a' and* ***R****'s private key is 'b'.*

V. SIMULATION & ANALYSIS

We compared our secure multi-path routing mechanism with the SRP [11], secure multi-path routing protocol of Burmester and Van Le [4] and SecMR [12] routing protocols. We perform the simulation of each of these security schemes. We have compared the routing overhead, data throughput of these schemes and also the amount of energy consumed by these schemes at each node.

A. Network & Communication Model

We performed the simulation in NS-2 [15]. The network model was consisted of 49 client nodes placed randomly within an area of 1000 x 1000 m^2. There are 16 mobile router nodes deployed in a grid environment to make up the mesh infrastructure. This scenario constructed 10 different mobile client networks. Each node has a propagation range of 150 meters with channel capacity 2 Mbps. The speed of mobile nodes is set to be 0 or 20 m/s. The size of the data payload is 512. Each run of simulation is executed of 900 seconds of simulation time. The medium access control protocol used is IEEE 802.11 DCF. The traffic used is constant bit rate (CBR). We have compared the protocols in different scenarios by using 15 data sources and different scalar inter-arrival time of data packets.

B. Results

Fig. 4 shows the routing overhead of the comparing routing protocols as a function of inter-arrival time. The Multipath protocol by Burmester and Van Le [4] has the highest routing overhead while the other three schemes have less overhead. SRP [11] has very little overhead as it only uses secret key cryptography to authenticate the end nodes. SecMR [12] and the proposed MHRP do not have much routing overhead as both these schemes separate the mutual authentication phase from the route discovery phase. We can observe from the graph in Fig. 4 that MHRP is little bit better than SecMR in discovering routes.

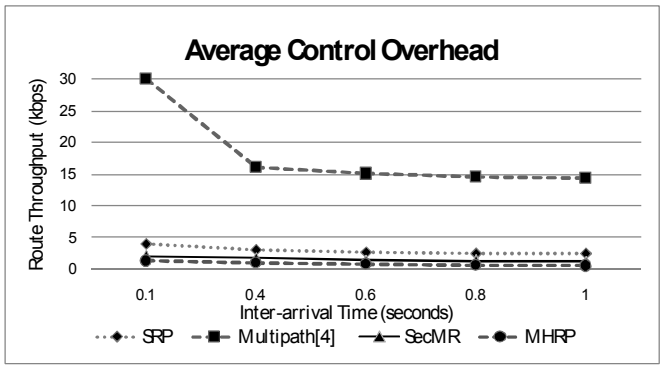

Figure 4. Routing overhead in terms of route throughput as a function of inter-arrival data packet's time.

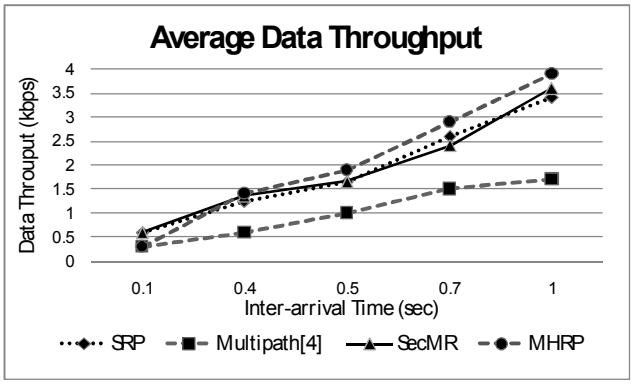

Figure 5. Data throughput as a function of inter-arrival data packet's time with 15 sources.

Fig. 5 shows the amount of data served by each protocol when 15 sources are generating data for different destinations. Multipath [4] has least throughput while other have better throughput. MHRP [4] has best data throughput among all the schemes.

Fig. 6 shows the energy consumption by the nodes running with different routing protocols in a similar simulation environment. Each node is provided with 5 joules of initial energy. As the nodes perform transmission and receive messages their energy level is decreased. Fig. 6 shows the energy levels at each node after the end of simulation of each scheme. The graph in Fig. 6 shows that [4] uses the amount of energy which means it has much higher amount of transmissions than other schemes. Among the other three schemes SRP is best after that our scheme is better than the SecMR protocol.

C. Simulation Analysis

From the results, we observe that SRP is the best scheme as it has less over head and nice data throughput and also consumes very little amount of energy. However, SRP does not provide optimal security; the intermediate nodes are not authenticated and the messages integrity is ensured

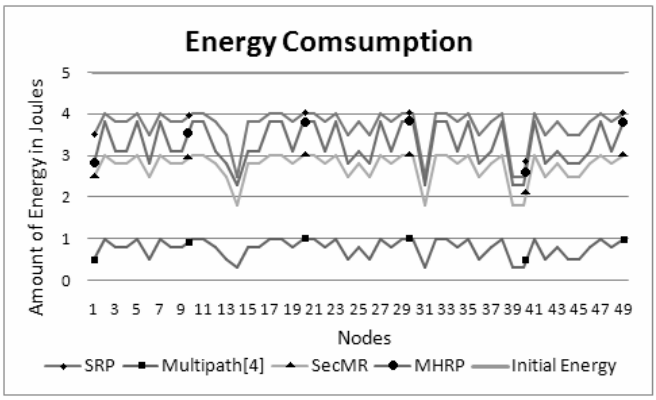

Figure 6. Amount of energy left in joules at each node after the 900 s simulation.

by secret key cryptography. All this factors sum up to make SRP not feasible for wireless mesh networks.

The high routing overhead of scheme in [4] is due to the fact that it attaches the neighborhood information along with digital signatures with the route request and forward it towards the destination node. This information is increased at every node so the message size increases drastically and produces a huge amount of overhead. This also reduces the data throughput, as more time is wasted in route discovery than in data transfer. Although [4] is good for security and provides mutual authentication between the intermediate nodes as well as the end nodes but its overhead is too much; lot of energy is required at the client nodes and a share of bandwidth is wasted, plus delay in finding the route is also very high.

SecMR protocol seems to be better than other schemes as it has less routing overhead and energy consumption than [4] and it also provides secure messaging with nice data throughput. In SecMR, each node mutually authenticates its neighbor node at a periodic interval and public key cryptography is used to ensure security of the messages. Although the routing phase is separated from this authentication phase but this authentication is required after a constant interval, hence a considerable amount of energy is wasted in these periodic mutual authentications. This also affects the data throughput.

MHRP does not require this periodic authentication, instead it uses public key cryptography only once and secret keys are used for further communication. This secret key deployment is not periodic and done after the mutual authentication by using public key cryptography. This reduces the energy consumption at each node and the routing overhead is also less than the other schemes. Therefore, less time is wasted in finding the route in MHRP plus it efficiently uses the characteristics of WMNs. By utilizing the resourceful router nodes in route discovery and security mechanism, it reduces the overhead

at the client nodes. Hence MHRP can provide better data throughput than other routing protocols.

D. Security Analysis

Our mechanism is secure enough that if a node is compromised then the whole network does not get affected by it. As all nodes communicates with each other with separate secret keys so, if a node is compromised and tries to adverse the network it is not possible for the node to be much hostile to the rest of the network. If there is a compromised node in the network, then there are two possibilities of an adversary node being in the network. In case 1, a node outside the network tries to attack the routing mechanism. Case 2 is the scenario in which the node entering the network is already a compromised node or the node is compromised during its participation in the network (such as due to the lack of physical protection etc). In the first case, the messages by the compromised node would not be accepted by the other nodes as it cannot be authenticated by them. So the adverse messages would be dropped by the nodes as they cannot verify the adverse node as a member node.

The second case can be harmful for the network as other nodes can verify the compromised node as a decent node. This node can communicate with its neighbor nodes and can inject false information in the network. But this compromised node cannot listen to other nodes' communications and cannot affect them. So if a node is compromised in the network all the other nodes are save from this node and can communicate with other nodes securely. As our mechanism is for a multi-path routing protocol, hence, the messages are secure from the adversary as there are several paths to evade the compromised nodes. Even if the adversary have *'n'* compromised nodes with every compromised node is in a different path then with *'m'* paths in between two nodes, adversary require $n \geq m$.

VI. CONCLUSION

In this paper, we have presented a secure multi-path routing protocol for wireless mesh network. Our routing scheme is hybrid in nature as it uses both proactive and reactive approach in finding the routes to the destination. Our security mechanism also sufficiently decreases the control overhead induced by a secure routing protocol. MHRP provide better data throughput with less route latency and overhead and consume less amount of energy at each node. It efficiently utilizes the characteristics of WMN to find alternate routes and provide reliable secure communication.

REFERENCE

[1] Bruno, R. Conti, M. Gregori, E. "Mesh networks: commodity multihop ad hoc networks", IEEE Communications Magazine, March 2005, Volume: 43, Issue: 3, pp: 123- 131.

[2] I. F. Akyildiz, X. Wang and W. Wang, 'Wireless Mesh Network: A Survey' in Computer Networks and ISDN Systems, Volume 47, Issue 4, March 2005.

[3] J. J. Garcia-Luna-Aceves and M. Mosko, "Multipath Routing in Wireless Mesh Networks", in first IEEE Workshop on Wireless Mesh Networks (WiMesh 2005); 2005 September 26; Santa Clara; CA.

[4] M. Burmester and T. van Le, Secure multipath communication in mobile ad hoc networks, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2004) (Las Vegas), IEEE, April 2004.

[5] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-demand Distance Vector (AODV) Routing", IETF RFC 3561, July 2003.

[6] S. Hamma, E. Cizeron, H. Issaka, and J.-P. Guédon, "Performance Evaluation of Reactive and Proactive Routing Protocol in IEEE 802.11 Ad hoc Network" in the proceedings of SPIE, Next-Generation Communication and Sensor Networks 2006, Volume 6387, October 2006.

[7] J. Broch, D. A. Maltz, D. B. Johnson, Y-C. Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols" in the proceedings of the Fourth Annual International Conference on Mobile Computing and Networking (MobiCom'98), Oct. 1998, pp: 85-97.

[8] A.A. Pirzada, C. Mcdonald and A. Datta, "Performance Comparison of Trust-based Reactive Routing Protocols" in IEEE Transactions on Mobile Computing, June 2006, Volume: 5, Issue; 6, pp. 695- 710

[9] Y. Ganjali and A. Keshavarzian, "Load Balancing in Ad hoc Networks: Single-path Routing vs. Multi-path Routing", in the proceedings of IEEE Annual Conference on Computer Communications (INFOCOM), March 2004, pp. 1120—1125.

[10] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks" Mobile Computing and Communications Review, Vol.6, No.4, October 2002

[11] P. Papadimitratos and Z. Haas, Secure routing for mobile ad hoc networks, In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS) (TX, San Antonio), January 2002.

[12] P. Kotzanikolaou, R. Mavropodi, and C. Douligeris, Secure multipath routing for mobile ad hoc networks, Proceedings of the WONSS05 Conference (St. Moritz, Switzerland), IEEE, January 19-21 2005, pp. 89–96.

[13] S. Raghani; D. Toshniwal; R. Joshi; "Dynamic Support for Distributed Certification Authority in Mobile Ad Hoc Networks" in the proceedings of ICHIT 2006, Volume 1, Nov. 2006 pp. 424 – 432.

[14] W. Diffie, P. van Oorschot, and M. Wiener. "Authentication and Authenticated Key Exchange. Designs, Codes and Cryptography, 2(2)", 1992, pp. 107–125.

[15] "UCB/LBNL/VINT Network Simulator - ns 2" URL: http://www.isi.edu/nsnamjns.