RESEARCH ARTICLE OPEN ACCESS

High Security Routing On Three-Hop

Sreekesh TU [1], Sreelakshmi k sunil [2]
Computer Science and Engineering
CISAT Moovattupuzha
Computer Science and Engineering
IES College of Engineering, Chittilapilly
Kerala

ABSTRACT
Both mobile ad-hoc networks and infrastructure wireless network combined together to form the Hybrid wireless network. It combines the advantages of both these two. Here, in this paper we are providing security to distributed three-hop routing protocol for hybrid wireless network. To take full advantage of the widespread base stations DTR divides a message data stream in to segments and transmit the segments in a distributed manner. It makes full spatial reuse of a system via its cellular interface. Furthermore, sending segments to a number of base stations simultaneously increase throughput and makes full use of wide spread base stations. In addition, DTR reduces overhead due to short path length and elimination of route discovery and maintenance. Here we introduce another technique called signcryption for efficient authentication. Signcryption used for data encryption and for creating digital signature. The major advantage of signcryption is that it involves lower computational cost than the sign-then-encryption process.

Keywords:- Signcryption, DTR

I. INTRODUCTION

Infrastructure wireless networks and mobile ad-hoc networks (MANETs) have developed very much today. The growing desire to increase wireless network capacity for high performance applications has stimulated the development of hybrid wireless networks. A hybrid wireless network consists of both an infrastructure wireless network and a mobile ad-hoc network. Wireless devices such as smart-phones, tablets and laptops, have both an infrastructure interface and an ad-hoc interface. As the number of such devices has been increasing sharply in recent years, a hybrid transmission structure will be widely used in the near future. Such a structure synergistically combines the inherent advantages and overcome the disadvantages of the infrastructure wireless network and mobile ad-hoc networks.

In a mobile ad-hoc network, with the absence of a Central control infrastructure, data is routed to its destination through the intermediate nodes in multi-hop manner .The multi-hop routing needs on-demand route discovery or route maintenance. Since the messages are transmitted in wireless channels and through Dynamic routing paths, mobile ad-hoc networks are not as reliable as infrastructure wireless networks. Further-more, because of the multi-hop transmission feature, mobile ad-hoc networks are only suitable for local area data transmission.

The infrastructure wireless network (e.g. cellular network) is the major means of wireless communication in our daily lives. It excels at inter-cell communication (i.e., communication between nodes in different cells) and Internet access. It makes possible the support of universal network connectivity and ubiquitous computing by integrating all kinds of wireless devices in to the network. In an infrastructure network, nodes communicate with each other through base stations (BSes).Because of the long distance one-hop transmission between BSes and mobile nodes, the infrastructure wireless networks can provide higher message transmission reliability and channel access efficiency, but suffer from higher power consumption on mobile nodes and the single point of failure problem.

A hybrid wireless network synergistically combines an infrastructure wireless network and a Mobile ad-hoc network to leverage their advantages and overcome their short comings, and finally increases the throughput capacity of a wide-area wireless network. A routing protocol is a critical component that affects the through-put capacity of a wireless network in data transmission. Most current routing protocols in hybrid wireless networks simply combine the cellular transmission mode (i.e.BS transmission mode) in infrastructure wireless networks and

the ad-hoc transmission mode in mobile ad-hoc networks. The protocols use the multi-hop routing to forward a message to the mobile gateway nodes that are closest to the BSes or have the highest band width to the BSes. The band width of a channel is the maximum throughput (i.e., transmission rate in bits/s) that can be achieved. The mobile gate way nodes then forward the messages to the BSes, functioning as bridges to connect the ad-hoc network and the infrastructure network

With the development of wireless technologies, Mobile services have dramatically increased to provide a more convenient life to people. Among these services, the roaming service allows mobile device users to use network services even when they reside in foreign domains .The basic roaming service involves a home server, a foreign server, and a roaming user. For secure roaming service, the foreign server must authenticate the roaming user, who originally subscribed to the home server. Hence, an authentication mechanism is an important requirement for providing secure roaming services.

Roaming services should be secure, i.e., provide authentication to identify legal roaming users' .As well as security, Location privacy should be provided to protect trajectories of roaming users. Research studies on privacy-preserving methods for protecting location information have been carried out .In particular; various anonymous authentication methods have been proposed to achieve secure authentication and location privacy simultaneously. According to, anonymous authentication could be classified in to two types: weak user anonymity authentication and strong user anonymity authentication. The former hides the user's identity only from third parties, such as general communication nodes (e.g., neighbor's mobile phones) or malicious nodes, whereas the latter hides the user's identity even from foreign servers, i.e., communication service providers that exist in foreign domains.

Roaming protocols could be divided in to two types: three-party protocols involving a home server and two-party protocols that do not involve a home server. In recent years, various three-party protocols have been proposed for anonymous authentication. These protocols require at least four rounds of communications in two rounds are required for a foreign server to acquire authentication information on a roaming user from a home server. It is also obvious that an authentication process in the three-party type is influenced by the state of the home server, which can be a bottle neck and a single point of a failure. Additionally, these protocols should open a communication connection between a foreign server and a home server without an authentication process whenever a roaming user requests roaming services, which could be exploited by an adversary to deplete resources of the foreign server. Recently, two-party roaming protocols that do not require the assistance of a home server during roaming have been proposed. Yang et al. Proposed two two-party roaming protocols. The first protocol fails to provide strong user anonymity, while these involve high computational costs when generating the group signature which is based on bi-linear pairing operations. In addition, the second protocol does not provide backward unlinkability, which means that the past protocol logs of a revoked user should remain anonymous and unlinkable, because a foreign server can trace the user's past information once a revoked user's revocation key is delivered to the foreign server.

To remedy these problems, He et al. proposed a roaming protocol based on a group signature with backward unlinkability that incurs high roaming authentication cost for the roaming user. For backward unlinkability, it provides each roaming user with N secret keys, where N is the system parameter .As N increases, the property of backward unlinkability becomes stronger. However, in this protocol, there vocation cost and revocation list size increase with the number of revoked users and N. This heavy checking operation could be exploited by an adversary to launch a resource depletion attack on the foreign servers. He et al. also proposed a pseudo-identity-based roaming protocol using bilinear pairing operations to provide foreign servers and roaming users with efficient cryptographic operations. Unfortunately, this protocol does not protect both private keys and session keys of roaming users from an adversary since the private keys and session keys can be computed from messages that can be obtained from simple eaves dropping.

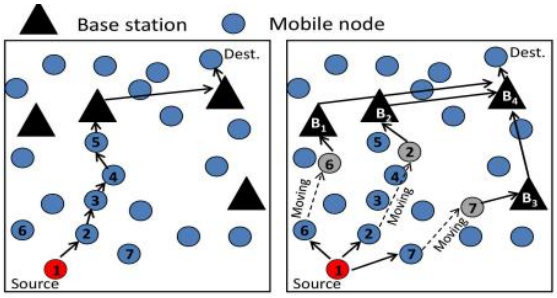

Figure 1: traditional vs three hop routing protocol

However, direct combination of the two transmission Modes inherits the following problems that are rooted In the ad-hoc transmission mode.

II. RELATED WORKS

In Hybrid wireless network protocols byRS Chang, WY Chen, YF Wen, Basically, there are two types of wireless network systems - base-station (BS) oriented networks and ad hoc wireless networks. In the first type, the mobile hosts communicate with base stations, while, in ad hoc networks, the mobile hosts communicate with one another directly. The BS-oriented wireless network has better performance and is more reliable. However, the ad hoc network topology is desirable because of its low cost, plug-and-play convenience, and flexibility. Its usage of bandwidth and battery power is more efficient, but route and communication connectivity is fairly weak; any migration by a host participating in one or more routes could make the route invalid. Much cost is incurred in maintaining communication. Thus, the ad hoc wireless network is only suitable for applications in a small geographical area. We propose hybrid wireless network protocols to combine the advantages of BS-oriented and ad hoc wireless networks. We allow two mobile hosts to communicate directly (one-hop direct transmission) or through another mobile host (two-hop direct transmission) within a BS- oriented network. The hybrid protocols are more flexible, reliable, and have better performance than the traditional protocols. Simulation results show that two-hop direct-transmission has a lower non- completion probability. If the communicating parties are always within a two-hop direct transmission area, the rate of complete communication improves by about 20%.

In the paper The capacity of hybrid wireless network by B.liu, Z.liu , and D.Towsley. The paper involves the study of the throughput capacity of hybrid wireless networks. A hybrid network is formed by placing a sparse network of base stations in an ad hoc network. These base stations are assumed to be connected by a high bandwidth wired network and act as relays for wireless nodes. They are not data sources nor data receivers. Hybrid networks present a tradeoff between traditional cellular networks and pure ad hoc networks in that data may be forwarded in a multi hop fashion or through the infrastructure. It has been shown that the capacity of a random ad hoc network does not scale well with the number of nodes in the system. In this work, we consider two different routing strategies and study the scaling behavior of the throughput capacity of a hybrid network. Analytical expressions of the throughput capacity are obtained. For a hybrid network of n nodes and m base stations, the results show that if m grows asymptotically slower than $\sqrt{n}$, the benefit of adding base stations on capacity is insignificant. However, if m grows faster than $\sqrt{n}$, the throughput capacity increases linearly with the number of base stations, providing an effective improvement over a pure ad hoc network. Therefore, in order to achieve non negligible capacity gain, the investment in the wired infrastructure should be high enough.

In hybrid network model for wireless packet data networks byH.Y Hsieh and R. Sivakumar It is a network model called Sphinx for cellular wireless packet data networks. Sphinx uses a peer-to-peer network model in tandem with the cellular network model to achieve higher throughput and lower-power consumption. At the same time, Sphinx avoids the typical pitfalls of the pure peer-to-peer network model including unfair resource allocation, and throughput degradation due to mobility and traffic locality. We present simulation results showing that Sphinx outperforms the cellular network model in terms of throughput and power consumption, and achieves better fairness and resilience to mobility than the peer-to-peer network model.

In the paper named Efficient resource allocation in hybrid wireless network proposed by B.Bengfort, W.Zhang and X.Du, we study an emerging type of wireless network - Hybrid Wireless Networks (HWNs). A HWN consists of an infrastructure wireless network (e.g., a cellular network) and several ad hoc nodes (such as a Mobile ad hoc network). Forming a HWN is a very cost-effective way to improve wireless coverage and the available bandwidth to users. Specifically, in this work we investigate the issue of bandwidth allocation in multi-hop HWNs. We propose three efficient bandwidth allocation schemes for HWNs: top-down, bottom-up, and auction-based allocation schemes. In order to evaluate the bandwidth allocation schemes, we develop a simulated HWN environment. Our simulation results show that the proposed schemes achieve good performance: the schemes can achieve maximum revenue/utility in many cases, while also providing fairness. We also show that each of the schemes has merit in different application scen

III. WHY DTR?

High overhead: Route discovery and maintenance incur high overhead. The wireless random access medium Access control (MAC) required in mobile ad-hoc networks, which utilizes control hand shaking and a back-off mechanism, further increases overhead.

Hotspots: The mobile gate way nodes can easily become hotspots. The RTS- CTS random access, in which most traffic goes through the same gateway, and the flooding employed in mobile ad-hoc routing to discover routes may exacerbate the hot spot problem. In addition, mobile nodes only use the channel resources in their route direction, which may generate hot spots while leave resources in other directions under-utilized. Hot spots lead to low transmission rates, severe network congestion, and high data dropping rates.

Low reliability: Dynamic and long routing paths lead to unreliable routing. Noise interference and neighbor Interference during the multi-hop transmission process causes a high data drop rate. Long routing paths increase the probability of the occurrence of path breakdown Due to the highly dynamic nature of wireless ad-hoc networks. These problems become an obstacle in achieving high throughput capacity and scalability in hybrid wireless networks. Considering the widespread BSes, the mobile nodes have a high probability of encountering a BS while moving. Taking advantage of this feature, we propose a Distributed Three-hop Data Routing protocol(DTR).In DTR, as shown in Figure1(b), a source node divides A message stream in to a number of segments. Each Segment is sent to a neighbor mobile node. Based on The QoS requirement, these mobile relay nodes choose between direct transmissions or relay transmission to the BS.

In relay transmission, a segment is forwarded to another mobile node with higher capacity to a BS than The current node. In direct transmission, a segment is directly forwarded to a BS. In the infrastructure, the Segments are rearranged in their original order and sent to the destination. The number of routing hops in DTR is confined to three, including at most two hops in the ad-hoc transmission mode and one hop in the cellular transmission mode. To overcome the aforementioned short comings, DTR tries to limit the number of hops. The first hop forwarding distributes the segments of a message in different directions to fully utilize there sources, and the possible second hop forwarding ensures the high capacity of the forwarder. DTR also has a congestion control algorithm to balance the traffic load between the nearby BSes in order to avoid traffic congestion at BSes. Using self-adaptive and distributed routing with high-Speed and short-path ad-hoc transmission, DTR significantly increases the throughput capacity and scalability of hybrid wireless networks by overcoming the three Short comings of the previous routing algorithms.

DTR has the following features:

Low overhead: It eliminates overhead caused by route Discovery and maintenance in the ad-hoc transmission mode, especially in a dynamic environment.

Hot spot reduction: It alleviates traffic congestion at mobile gateway nodes while makes full use of channel resources through a distributed multi-path relay

High reliability: Because of its small hop path length with a short physical distance in each step, it alleviates Noise and neighbor interference and avoids the adverse effect of route break down during data transmission. Thus, it reduces the packet drop rate and makes full use of special reuse, in which several source and destination nodes can communicate simultaneously without interference.

Since BSes are connected with a wired back bone, we assume that there are no band width and power constraints On transmissions between BSes .We use intermediate nodes to denote relay nodes that function as gateways Connecting an infrastructure wireless network and a Mobile ad-hoc network .We assume every mobile node is dual-mode; that is, it has ad-hoc network interface such as a WLAN radio interface and infrastructure network interface such as a 3G cellular interface. DTR aims to shift the routing burden from the ad hoc network to the infrastructure network by taking Advantage of widespread base stations in a hybrid wireless network. Rather than using one multi hop path to forward a message to one BS, DTR uses at most two hops to relay the segments of a message to different BSes in A distributed manner, and relies on BSes to combine the segments. Figure2 demonstrates the process of DTR in a hybrid wireless network.

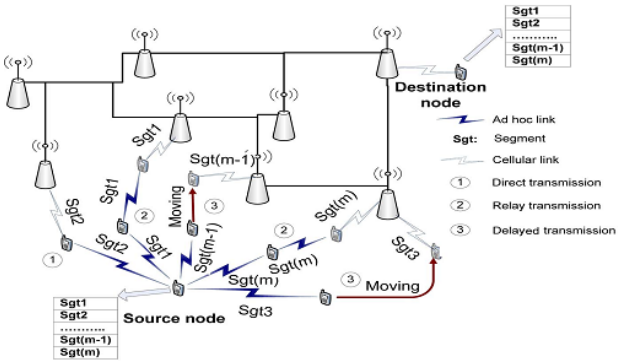

Figure 2: data transmission in DTR

We simplify the routings in the infrastructure network for clarity. As shown in the figure, when a source node wants to transmit a message stream to a destination node, it divides the message stream in to a number of partial streams called segments and transmits each segment to a neighbor node. Upon receiving a segment from the source node, a neighbor node locally decides between direct transmission and relay transmission based on the QoS requirement of the application. The neighbor nodes forward these segments in a distributed manner to nearby BSes. Relying on the infrastructure network routing, the BSes further transmit the segments to the BS where the destination node resides. The final BS rearranges the segments in to the original order and forwards the segments to the destination. It uses the cellular IP transmission method to send segments to the destination if the destination moves to another BS during segment transmission.

Our DTR algorithm avoids the short comings of ad-hoc transmission in the previous routing algorithms that directly combine an ad-hoc transmission mode and a Cellular transmission mode. Rather than using the multi-Hop ad-hoc transmission, DTR uses two hop forwarding By relying on node movement and widespread base stations. All other aspects remain the same as those in the previous routing algorithms (including the interaction with the TCP layer). DTR works on the Internet layer. It receives packets from the TCP layer and routes it to the destination node, where DTR forwards the packet to the TCP layer.

The data routing process in DTR can be divided in to two steps: uplink from a source node to the first BS and downlink from the final BS to the data's destination. Critical problems that need to be solved include how a source node or relay node chooses nodes for efficient segment forwarding, and how to ensure that the final BS sends segments in the right order so that a destination Node receives the correct data. Also, since traffic is not evenly distributed in the network, how to avoid Overloading BSes is another problem.

IV. PERFORMANCE EVALUATION

This section demonstrates the properties of DTR through Simulations on NS-2 in comparison to D Hybrid, Two-hop and AODV. In D Hybrid, a node first uses broad casting to observe a multi-hop path to its own BS and then forwards a message in the ad-hoc transmission mode along the path. During the routing process, If the transmission rate(i.e., band width)of the next hop to the BS is lower than a threshold, rather than forwarding the message to the neighbor, the node forwards the message directly to its BS. The source node will be notified if an established path is broken during data transmission. If a source sends a message to the same destination next time, it uses the previously established path if it is not broken. In the Two-hop protocol, a source node selects the better transmission mode between direct transmission and relay transmission. If the source nodes can find a neighbor that has higher band width to the BS than itself, it transmits the message to the neighbor. Otherwise, it directly transmits the message to the BS.

SCALABILITY

DTR uses distributed multi-path routing to fully take advantage of the spatial reuse and avoid transmission congestion in a single path. Unlike the multi-hop routing in mobile ad-hoc networks, DTR does not need Path query and maintenance. Also, it limits the path Length to three to avoid problems in long-path transmission. The throughput of D Hybrid and AODV decreases as the number of nodes in the network increases. This is mainly because when the network size increases, more beacon messages are generated in the network. Also, the long transmission path also leads to high transmission interference. Then, nodes in these methods suffer from intense interference, leading to more transmission failure and degraded overall throughput. Also, the mobile node increase in the system leads to high network dynamism, resulting infrequent route re-establishments.

Transmission delay

Transmission delay is the amount of time it takes for a message to be transmitted from its source node to its destination node. From the figure, we see that DTR Generates the smallest delay. In DTR, each source node first divides its messages in to smaller segments and then forwards them to the nearby nodes with the highest capacity, which leads to more balanced transmission load distribution among nodes than the previous methods. Average latency can be minimized when the transmission loads of all the nodes are balanced. Hence, DTR has smaller latency than the previous methods. The delay of D Hybrid is 5-6 times larger than DTR. D Hybrid uses a single transmission path, while DTR uses multiple paths. Recall that we set the number of segments of a message to the connection degree of the source node in DTR. Thus, the ratio of delay time of D Hybrid to that of DTR equals the average connection degree. As the number of nodes in the system increases, the connection degree of each node

increases, and the increase rate of the ratio grows. This is caused by two reasons. First, a higher node density leads to longer path lengths in D Hybrid, resulting in a longer delay because of a higher likelihood of link breaks. Second, a higher node density enables a node to quickly find relay nodes to forward messages in DTR.

Communication Overhead

We use the generation rate of control messages in the network and MAC layer sink bp store present the communication over head of the routing protocols. We can see that the communication overheads of DTR and two-hop are very close. This is because both DTR and two-hop are transmission protocols of short distance and small hops. DTR has slightly higher communication overhead than Two-hop because DTR utilizes three hop transmission, which has one more hop than two hop transmission. However, the marginal overhead increase leads to a much higher transmission through put .D Hybrid generates much higher overhead than DTR and Two-hop because of the high overhead of routing path querying .The pure AODV routing protocol results in much more overhead than the others. This is because without an infrastructure network, the messages in AODV travel along way from the source node to the destination node through much longer paths.

Effect of Mobility

In order to see how the node mobility influences the Performance of the routing protocols, we evaluated the throughput of these four transmission protocols with different node motilities. It is intriguing to find that high mobility can even help DTR to increase its throughput and that Two-hop generates constant throughput regardless of the mobility. This is because the DTR and Two- hop transmission modes do not need to query and rely on multi-hop paths; thus, they are not affected by the network partition and topology changes. Moreover, since DTR transmits segments of a message in a distributed manner, as the mobility increases, a mobile node can meet more nodes in a shorter time period. Therefore, DTR enables the segments to be quickly sent to high- capacity nodes. As node mobility increases, the throughput of D Hybrid decreases. In D Hybrid, the messages are routed in a multi-hop fashion. When the links between nodes are broken because of node mobility, The messages are dropped. Therefore, when nodes have smaller mobility, the links between the mobile nodes last longer and more messages can be transmitted. Hence, The throughput of D Hybrid is adversely affected by node mobility. However, since D Hybrid can adaptively adjust the routing between the ad-hoc transmission and cellular transmission, the throughput of D Hybrid is much higher than AODV's. With no infrastructure network, AODV produces much lower through put than the others. Its throughput also drops as node mobility increases for the same reasons as D Hybrid.

Effect of Work load

We measured the total throughput of BSes on the messages received by BSes. we can see that DTR and Two-hop have much higher throughput increase rates than D Hybrid. This is because in DTR and Two-hop, the number of transmission hops from a source node to a BS is small. Meanwhile, each node can adaptively switch between relay transmission and direct transmission based on the transmission rate of its neighbors. Hence, part of a Source node's transmission load is transferred to a few Relay nodes, which carry the messages until meeting the BSes. Therefore, the gateway mobile nodes are less likely to be congested. However, nodes in D Hybrid cannot adaptively adjust the next forwarding hop because it is Predetermined in the routing path. Messages are always forwarded to the mobile gateway nodes that are closer To the BSes or that have higher transmission rates. Therefore, these mobile gateway nodes can easily become congested as the workload of the system increases, leading to many message drops. Therefore, when the number of the source nodes is larger than 4, the throughput of D Hybrid remains nearly constant. This is also the reason that the through put of D Hybrid is constantly lower than those of DTR and Two-hop. Additionally, the figure shows that the overall throughput of two-hop is lower than that of DTR. This is because most of the traffic in two-hop is confined to a single cell. When a BS in a cell is congested, the traffic cannot be transferred to other cells. In contrast, DTR's three-hop distributed forwarding mechanism enables it to distribute the traffic among the BSe in a balance. Therefore, the BSes in DTR will not become congested easily. In addition, as the forwarding mechanism gives nodes more flexibility in choosing relay nodes with higher transmission rates for message forwarding to the BSes, the overall BS through put in DTR is larger than in two-hop.

Effect of the Number of Routing Hops

We conducted experiments to show the optimal number of routing hops for the routing in hybrid wireless networks. We tested the through put per S-D pair for x-hop DTR, where x was varied from 1 to 4. In the 1- hop routing, a node directly transmits a message to the BS without message division. In the other routing protocols,

the (x 1) th hop chooses the best transmission mode between direct transmission and relay transmission. Also, in the 4- hop routing, the second relay node randomly chooses the third relay node.

Load Distribution within a Cell

In this experiment, we tested the load distribution of mobile nodes in a randomly chosen cell in the hybrid wireless network that employs each of the DTR, D Hybrid, and Two-hop protocols. We normalized the distance from a mobile node to its base station according to the function D, Rb, where D is the actual distance and Rb is the radius of its cell. We divided the space of the cell in to several concentric circles and measured the loads of the nodes on each circle to show the load distribution.

V. SECURITY MECHANISMS

Anonymity

Our protocol provides roaming users with strong user anonymity. We use pseudo-identities that are not related to the real identities of the roaming users. However, if legal issues arise, The corresponding real identity can be traced.

Backward Unlinkability

To protect trajectories of roaming users using linkable information, the protocol is designed such that there is no relation among pseudo-identities .Even if are vocation value of a revoked roaming user is revealed ,the user's past pseudo-identities are not linked.

Revocation cost

There vocation cost of Yang etal.'s second protocol includes pre-computation and two pairing operations, while He etal.'s protocol involves a huger evocation cost. However, our revocation process requires only a few hash operations. We use a keyed hash chain to revoke malicious users.

Authentication cost

The authentication cost for roaming services can be divided in to two parts : cost at the roaming user and cost at the roaming server. In our authentication process, a roaming user performs only 6.5 elliptic curve multiplications. However, Yangelal.'s second protocol requires three pairing oper-ations and 8.75 elliptic curve multiplications, while He etal.'s protocol requires four pairing operations and 16.75 elliptic curve multiplications. Taking the roaming authentication cost of a foreign server in to account , our protocol, which supports a fast revocation process, is more cost efficient than those proposed

Revocation list size

The protocol consumes a large amount of communication band width since the revocation values of all revoked users should always be included in the revocation list. However, in our revocation list, one hash element and a revocation key of a revoked user appear only once, because our revocation method uses a hash chain. Storage capacity of Subscriber Identification Module (SIM) card: We use pseudo-identities to provide anonymity. In general, methods that use pseudo identities without the periodic assistance of the home server require a huge storage capacity to store large number of pseudo-identities. However, in the roaming environment, these methods should take in to account the limited storage capacity of a SIM card, since a roaming user may change his or her mobile device while roaming. In our protocol, we minimize the number of pseudo-identities to be stored on the SIM card by using signcryption.

Signcryption

Signcryption schemes are used for data encryption and for creating digital signatures. A major advantage of signcryption is that it involves lower computational cost than the sign-then-encryption process. This primitive assures message confidentiality and signature unforgeability. In addition, signcryption satisfies the cipher text anonymity property, and thus provides greater privacy. Cipher text anonymity means that cipher text must not include information about the identity of both the sender and the receiver. Our protocol uses a signcryption scheme to provide roaming users with anonymity and unlinkability by signcrypting roaming authentication requests, which contain the pseudo-identities of roaming users.

VI. CONCLUSION

It is an efficient protocol, because it provides both the faster transmission and security. That means this protocol or mechanism is reliable than any other protocols. It also reduces the hotspots and high overhead. It has both the encryption and signature security so it is doubly stronger. This method we implemented here is called Signcryption. So main advantage of this is we can transmit high confidential data reliably and quickely.

REFERENCES

[1] HLuo, R.Ramjee, P.Sinha, L.Li, and S.Lu.Ucan: A unified cell And ad-hoc network architecture. In Proc.of MOBICOM, 2003.

[2] P.K.McKinley, H.Xu, A.H.Esfahanian, and L.M.Ni. Unicast-Based multicast communication in wormhole-routed direct networks. TPDS,1992.

[3] H.Wu, C.Qiao, S.De, and O.Tonguz. Integrated cell and adhoc Relaying systems: iCAR. J-SAC,2001.

[4] Y.H.Tam, H.S.Hassanein, S.G.Akl, and R.Benkoczi. Optimal multi-hop cellular architecture for wireless communications. In Proc.ofLCN,2006.

[5] Y.D.Linand Y.C.Hsu. Multi-hop cellular: A new architecture For wireless communications. In Proc.ofINFOCOM,2000.

[6] P.T.Oliver, Dousse, and M.Hasler. Connectivity in adhoc and Hybrid networks. In Proc.ofINFOCOM,2002.

[7] E.P.Charles and P.Bhagwat. Highly dynamic destination Sequenced distance vector routing(DSDV)for mobile computers. In Proc.ofSIGCOMM,1994.

[8] C.Perkins, E.Belding-Royer, and S.Das. RFC3561:Adhoc On demand distance vector(AODV) routing. Technicalreport, Internet Engineering Task Force, 2003.

[9] D.B.Johnson and D.A.Maltz. Dynamic source routing in ad hoc wireless networks. IEEEMobileComputing,1996.

[10] V.D.Parkand M.Scott Corson. A highly adaptive distributed Routing algorithm for mobile wireless networks. In Proc. of INFOCOM,1997.

[11] R.S.Chang, W.Y.Chen, and Y.F.Wen. Hybrid wireless network protocols. IEEE Transaction on Vehicular Technology,2003.

[12] G.N.Aggelou and R.Tafazolli. On there laying capacity of next generation gsm cellular networks. IEEE Personal Communications Magazine,2001.

[13] T.Rouse, I.Band, and S.McLaughlin. Capacity and power Investigation of opportunity driven multiple access(ODMA) Networks in TDD-CDMA based systems. In Proc.of ICC,2002.

[14] H.Y.Hsieh and R.Sivakumar. On Using the Ad-hoc Network Model in Wireless Packet Data Networks. In Proc.of MOBIHOC, 2002.