

CERIAS Tech Report 2004-106

Integrating Heterogeneous Wireless Technologies: A Cellular Aided Mobile Ad hoc Network (CAMA)

by B Bhargava, X Wu, Y Lu, W Wang

Center for Education and Research

Information Assurance and Security

Purdue University, West Lafayette, IN 47907-2086

Integrating Heterogeneous Wireless Technologies: A Cellular Aided Mobile Ad hoc Network (CAMA)

Bharat Bhargava, Xiaoxin Wu, Yi Lu, and Weichao Wang

Abstract—A mobile ad hoc network is a collection of wireless terminals that can be deployed rapidly. Its deficiencies include limited wireless bandwidth efficiency, low throughput, large delays, and weak security. Integrating it with a well-established cellular network can improve communication and security in ad hoc networks, as well as enrich the cellular services. This research proposes a cellular-aided mobile ad hoc network (CAMA) architecture, in which a CAMA agent in the cellular network manages the control information, while the data is delivered through the mobile terminals (MTs). The routing and security information is exchanged between MTs and the agent through cellular radio channels. A position-based routing protocol, the multi-selection greedy positioning routing (MSGPR) protocol, is proposed. At times due to the complicated radio environment, the position information is not precise. Even in these cases, the MT can still find its reachable neighbors (the association) by exchanging "hello" messages. This association is used in complement with the position information to make more accurate routing decisions. Simulation results show that the delivery ratio in the ad hoc network is greatly improved with very low cellular overhead. The security issues in the proposed architecture and the corresponding solutions are addressed. The experimental study shows that CAMA is much less vulnerable than a pure ad hoc network.

Index Terms—heterogeneous networks, ad hoc networks, cellular networks, quality of service, security

I. INTRODUCTION

Future wireless technology aims at providing an umbrella of services to its users. Ad hoc networks have become attractive for their potential for commercial applications. Routing in ad hoc network is a challenge due to the mobility of users and the lack of central control. Different routing protocols are proposed in [8],[36],[37],[43]. These approaches suffer in network performance that includes large routing overhead, low throughput, and large end-to-end delay. In ad hoc networks, the issues of quality of service (QoS) [39] and security [50] are even more complicated because of the lack of reliable methods to distribute information in the entire network.

The integration of heterogeneous wireless technologies can improve the network performance, thereby meeting the demands for different quality of service (QoS). This research proposes a novel integrated architecture, called the cellular aided mobile ad hoc network (CAMA), to improve ad hoc networks. The architecture uses the idea of "out-of-band signaling" (over a cellular network). This enables an ad hoc network to improve the quality of network control and management. An analogy can be drawn to the Signaling System 7 (SS7), a common architecture for out-of-band signaling in support

of the call-establishment, billing, routing, and information-exchange functions of the public switched telephone network [14]. Another important feature of the proposed architecture is the availability of global information for the entire ad hoc network.

A typical CAMA architecture is shown in Figure 1. It is operated in places where a mobile ad hoc network overlaps a cellular network. The servers that are in charge of operating CAMA, called CAMA agents, are deployed in the cellular network. Each CAMA agent covers a number of cells and knows which mobile ad hoc user (MT) is a registered CAMA user. To get more user information, an agent should be connected with a home location register (HLR). These agents collect information for the entire ad hoc network and are involved in its authentication, routing, and security. MTs may contact the CAMA agents through the cellular network's radio channels to exchange the control information. As the CAMA agent can work as a position information server, positioning routing will be applied in this architecture.

CAMA is operated in areas well covered by a cellular network, such as metropolitan areas. The centralized CAMA agent is an easy solution for authentication, authorization, and accounting (AAA) in ad hoc networks, yet AAA is very difficult to implement in the pure ad hoc networks. Lack of AAA has been a major obstacle for commercial ad hoc networks. On the other hand, low-cost, high-data-rate ad hoc channel is suitable for wireless multimedia services. These services over the ad hoc channel can be supplementary to the normal cellular network services. Other than peer-to-peer communications in CAMA ad hoc networks, special MTs can also act as Internet access points, through which other MTs can connect to the IP network, instead of through expensive cellular channels. The additional load of control to the cellular network is compensated by the profits generated by the integrated network.

The proposed architecture is different from wireless LANs [2], [11]. In WLAN, all the control and data packets have to go through fixed access points. In CAMA, only control data goes through a cellular base station, while all other data is kept in the ad hoc network.

CAMA is different from the ad hoc networks with fixed nodes (i.e., server access points), which act as base stations. In such an ad hoc network, the mobile ad hoc users might have no idea whether a fixed node has joined the network or not. The fixed nodes are difficult to access because they have the same wireless channel coverage as the mobile ad hoc users.

CAMA can greatly improve ad hoc routing and security by using efficient out-of-band signaling and centralized control.

Xiaoxin Wu is with Department of Computer Sciences, Purdue University. Contact: wu@cs.purdue.edu

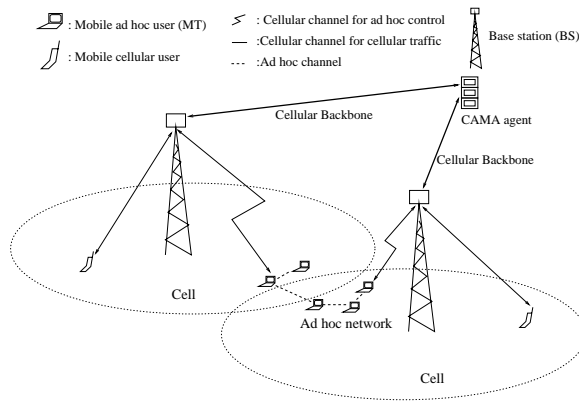


Fig. 1. Cellular-aided mobile ad hoc network.

These are discussed in the following sections. In addition, CAMA can improve the ad hoc network in:

- **Synchronization** The clock for all ad hoc users can be adjusted according to that of the cellular network in one step.
- **Authentication** In CAMA, MTs can go through the same authentication procedure as in cellular networks. The MTs can also be authenticated by special MTs, which can be reached easily by an entrant MT through the cellular radio channel.
- **Power saving** The transmitting power of MTs can be estimated since the distance between any two MTs is known. Additionally, in any new route discovery, the intermediate MTs need not receive and forward routing packets.
- **Radio resource allocation** The centralized CAMA agent can guide MTs to access the proper ad hoc channels in networks which have more than one ad hoc channel.
- **Broadcasting and multi-casting** Data can be sent to the base station (BS), and broadcast or multicast through the cellular radio channel. No further data forwarding is needed.
- **Finding cluster head in clustered ad hoc routing** In clustered ad hoc routing [27] [29], the CAMA agent can determine the cluster heads since it has the information of MTs, e.g., positions, stability, and power. On the other hand, clustered routing may improve CAMA. The CAMA agent has to communicate only with cluster heads, thus reducing the load in the cellular network.

CAMA is very feasible. Compared to the size of a cell in a normal cellular network, the size of an ad hoc network is relatively small because of the shorter transmission distance. It is probable that one cell covers an entire ad hoc network. This makes the operation fairly easy because all the MTs have to connect to only one BS. It is also possible for a cell to cover more than one ad hoc network. For larger ad hoc networks which cross more than one cellular cell, the CAMA agent can collect the information from all BSs involved.

The UMTS network has synchronization and broadcast channels. These can be directly used by the proposed architecture. UMTS also has up-link and down-link common-share channels for short messages. MTs may use these channels

to exchange information with the CAMA agents. For a 2G cellular network (e.g., GSM), a number of channels can be reserved for CAMA implementations.

Today's semiconductor design technology makes building mobile terminals that carry multiple transmitters and receivers quite easy. Mobile terminals can also run different protocols. On the other hand, it is common for different networks or operators to cooperate with each other in providing a certain service. An example is the global roaming service for a cellular user. There should be no problem for the future ad hoc network to cooperate with the cellular network in service management (e.g., billing).

Additionally, the services provided by cellular networks are no longer restricted to voice services. The new business models in international mobile telecommunication (IMT) enable cellular users with a simple user ID to get authorized to use different services on different mobile terminals (if needed). The ad hoc service can be added to the original phone service without assigning the user another user ID.

The rest of the work is organized as follows. In section II, we briefly review the previous work related to integrated networks, positioning routing, and security. In section III, we describe the positioning routing in CAMA. In section IV, we go through some security issues. In section V, we show the major simulation results. In section VI, we conclude our work.

II. PREVIOUS WORK

A. Heterogeneous Integrated Wireless Networks

Heterogeneous integrated wireless networks have been widely applied and studied. Examples of application of integrated technology are AMPS/IS-95 cellular network, global positioning system (GPS) applied in cellular network to provide position services, and satellite/cellular network [15], [42]. There is also a growing interest in the integration of cellular network and wireless LAN (WLAN). The Universal Mobile Telecommunication System (UMTS) [12], [20], [41], also called the 3G cellular network, is able to provide different services (voice and data services) on its own. However, due to the limited radio bandwidth, the network cannot accommodate a large number of users simultaneously, especially for applications requiring fast data transmission rate. In addition, the service cost is high. As a supplement to the cellular network, WLAN may provide services with high transmission data rate at a relatively low cost. The integration of these two heterogeneous networks can provide better service by having mobile users handoff back and forth between the networks to get the desired services [33], [38] and [47]. However, WLAN has a very small radio coverage (especially in urban areas) and can only provide services to users very close to its fixed access points. To be able to serve most of the users in such an integrated network, a high density of WLAN access points have to be deployed. This leads to the increased cost and reduced efficiency of the fixed infrastructure. To overcome this drawback, an ad hoc network can be used instead of WLAN. In the ad hoc/cellular integrated network, multi-hop ad hoc links virtually extend the radio coverage. The mobile users outside the radio coverage of service access points (fixed or

mobile) can also be accessed through intermediate forwarding. Peer-to-peer service can be achieved directly through the ad hoc network without going through the cellular network. Additionally, the ad hoc channels may be used to forward traffic between cells to get load balancing in the cellular network. This further improves the cellular network's capacity. The research of integrated ad hoc/cellular network can be found in [17], [45], and [46]. These works focus on how ad hoc network may enhance cellular services. The approach may be called ad hoc aided cellular networks.

B. Ad hoc Routing with Positioning Information

The global positioning system (GPS) [1], [35] has been widely used for positioning service. Based on the received satellite signals, an object may determine its own position through the built-in GPS chip. With the help of GPS, a source MT may know where the destination MT is and make the proper routing decision. Such a routing method is called a GPS-aided positioning routing. A greedy perimeter stateless routing (GPSR) protocol is studied in [10]. In GPSR, The next hop of a route is always the MT closest to the destination. An MT needs to know the precise position of all the other MTs. The authors make an assumption that there exists a position server. In [22], a source MT is assumed to know the position of the destination MT. Routing requests are not flooded in the network, but forwarded only towards the destination to reduce the routing overhead. In [19], a positioning routing protocol similar to that in [22] is studied. Other works on GPS aided routing can be found in [26][28].

Position management is studied in detail in [7],[25]. In [25], a distributed location server model is described. An MT uses other MTs within a certain area as its location servers. The MT will send its position to these location servers periodically. Other MTs can know this MT's position by reaching any of its location servers. In another location management approach [7], each MT has a virtual home region (VHR) with a fixed center. An MT updates its position by sending position advertisements to its VHR. In both papers, MTs have to know the approximate coverage of the ad hoc network. There is a relatively large overhead for location updates.

In an environment where GPS is not available, such as an indoor office, relative positioning information can be used by the ad hoc network to determine routing. A self positioning algorithm is used to calculate the relative positions for MTs in [7], so that a network coordinate system can be built for location information. In another paper [43], the authors propose a routing technique based on the association among ad hoc users instead of the precise locations. This routing protocol is called association beaconing routing (ABR) protocol. In most existing ad hoc routing protocols, there is a "hello" message that may help an MT get information about its neighbors. Yet it is difficult to achieve link-state routing in ad hoc networks because of the dynamic topology and slow information distribution.

In previous works, there is no specified centralized server providing global information, so a positioning routing based on the precise global position information can not be applied.

C. Security

Ad hoc networks are particularly vulnerable to attacks. This is due to its features of open medium, dynamic changing topology, cooperative algorithm, lack of centralized monitoring and management point, and the lack of a clear line of defense. Security in a pure ad hoc network also suffers from the slow information distribution, i.e., MTs may not be informed about an attack even after the attack has been discovered for some time. Security in ad hoc network can be achieved in two ways: 1)By preventing the ad hoc network from attacks (pro-active security) and 2)By detecting the intruders or malicious users and excluding them from the network (reactive security). The research for the pro-active security is mainly about key implementation and distribution. The research for the reactive security is mainly about the architecture to monitor the network, the information to be collected for intrusion detection, and the proper reactions to attacks.

Some general issues and proposed solutions for security in ad hoc network can be found in [21]. In [4] and [16], the ad hoc group key distribution without any certification authority (CA) is described. The efficiency of the key establishments is also studied in [4]. However, these key distribution schemes only work for small ad hoc user groups, where users can contact directly with each other. In [23], [40] and [50], the threshold cryptography (see [13]) is proposed for ad hoc key management. A user can only recover the key after it contacts a number of key servers (or key-share holders). This improves the network's robustness since the danger of one compromised key server destroying the overall key management system is excluded. Yet there may be key assignment failure, and assigning proper key servers is not an easy task in ad hoc network. In [18], a decentralized key agreement scheme is studied. Each MT has a trusted group around itself. Two MTs exchange their public keys by merging their trusted groups, thus each MT does not have to keep the public keys for all the other MTs. The drawback of this scheme is that there may be key agreement failures, especially in larger ad hoc networks.

In ad hoc networks, routing is a major security concern. In [34], a security association between the MT initiating the routing query and the sought destination MT is built by using message authentication code. Two mechanisms are used to secure AODV routing messages in [48]: digital signatures to authenticate the non-mutable fields of the messages, and hash chain to secure the hop count information. Both schemes in [34] and [48] aim at preventing the intermediate MTs from adding false routing information based on the assumption that there is a previous key agreement between the source and destination. An authenticated link-level routing protocol is proposed in [6] to secure the binding of IP addresses and MAC addresses in ad hoc networks.

For reactive security, a general architecture for intrusion detection in ad hoc network can be found in [49]. Each MT has its own intrusion detection system to monitor its local environment, and at the same time, to exchange the intrusion information with its neighboring MTs. The overall intrusion detection system is complicated and it depends on the trust

between the neighboring MTs. A similar intrusion detection architecture is discussed in [3].

There is routing misbehavior when the malicious MTs may drop, modify, or misroute packets in an attempt to disrupt the routing service. In [5], such routing misbehavior can be mitigated by an adaptive probing technique used to identify the exact fault link in a multi-hop routing failure. In watch dog scheme [30], an MT listens to its next hop MT to make sure it forwards its packets correctly. This consumes more power because an MT has to receive the same packet twice, i.e., from both its previous hop and its next hop. In [9], a protocol similar to the watch dog protocol, the Grudge-bird protocol, is proposed to improve the security for dynamic source routing (DSR) protocol. The vulnerability and protection in ad hoc on demand vector routing (AODV) protocol is investigated in [44]. In all the related works, the reaction of the intrusion detection is to exclude the malicious MTs (links) from routing or network services.

Previous research has pointed out the difficulty in enhancing security in an ad hoc network. This is because of lack of the centralized CA and security control point in a pure ad hoc network. The distributed security architecture can improve the ad hoc network security. However, the tradeoff is long decision time, increased network overhead, and inaccurate security judgment.

III. POSITIONING ROUTING IN CAMA

A. Centralized Positioning Routing

In CAMA, positioning routing is more feasible since the CAMA agent may work as a centralized positioning information server. An MT can find its precise geographical position through GPS¹. The position information is sent to the CAMA agent through the BS. An MT's position can also be found by the cellular network using the recent cellular position service. Distinct from the positioning routing used in the pure ad hoc network, in CAMA routing, the current position of each MT can be well known. An initial route from a source to a destination can thus be determined either by CAMA agents or by MTs. If the routing is determined by MTs, the BS will have to broadcast the most updated position information. Based on the received information, each MT makes its own routing decision.

In this work, CAMA agent is considered to be making the routing decision. Compared to MTs, the CAMA agent has more complete global information for the entire ad hoc network. This centralized routing mechanism also brings advantages of routing optimizations, security, radio resource allocation and power savings. Additionally, the centralized routing scheme does not need the periodic downlink broadcasting of the positioning information which normally consumes large cellular radio bandwidth and MT power. However, the centralized control has its disadvantage. An MT may have to wait for a long time to get the routing decision from the CAMA agent if too many MTs send routing requests at the same time. The delay is mainly caused by the backoff

¹The future 3G cellular network services include MT position service. However, in this paper, we focus on GPS.

MT A: A (x, y, z)

Neighboring MT	Position	d	Δd
B	B (x, y, z)	d_{AB}	Δd_{AB}
E	E (x, y, z)	d_{AE}	Δd_{AE}
F	F (x, y, z)	d_{AF}	Δd_{AF}
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮

Fig. 2. Routing table for MT A.

delay due to the uplink transmission collision. In the case of a CAMA agent serving MTs from more than one cell, the delay also includes the uplink request queuing delay and the downlink reply queuing delay. If the downlink delay is too high, the route may lose its contemporariness. A new route has to be determined by the updated position information. From the point of view of security, the centralized routing decision scheme may suffer the attack of denial of service (DoS).

In a real wireless network, especially in the urban area, two geographically close MTs may not reach each other via radio due to the complex radio propagation environment (e.g., radio block). To improve the GPS routing correctness, MTs can send “hello” messages to their neighbors to make sure they are reachable to each other (see method in [43]). This association information is sent to the CAMA agent with MTs' precise positions, so that the CAMA agent may know exactly what link exists, and make more accurate routing decisions. This, however, increases the overhead in both the cellular network and the ad hoc network. It should be noted that based on association between MTs, the CAMA agent may also make the routing decisions through link state routing methods (e.g., shortest path open first (OPSF)). The method is not as straight forward as GPS positioning routing and will be studied in our future work.

B. Routing Algorithm: Multi-Selection Greedy Positioning Routing (MSGPR)

For each MT, the CAMA agent keeps the position information table (shown in Figure 2). The table includes this MT's position, the IDs of its neighboring MTs within its radio coverage, the positions of its neighboring MTs, the distance d from the MT to its neighboring MTs, and Δd , the change of distance between the MT and its neighboring MTs based on the last two position updates. An MT's neighbors can be its next hop only when $d + \Delta d \leq d_\tau$, where d_τ is a distance threshold value within which two MTs can build a link with a required quality. This table is updated whenever there is a position update for any of the members in the table.

It is shown in [24] that GPSR may not find the best route. Additionally, GPSR considers the distance as the only routing judgment criteria. A novel routing algorithm—the multi-selection greedy positioning routing (MSGPR) algorithm—is proposed for GPS-aided position routing when using CAMA. In MSGPR, for a resource MT, n of its neighboring MTs which are closest to the destination are found at the beginning, as its next hops. These n MTs form an original searching set.

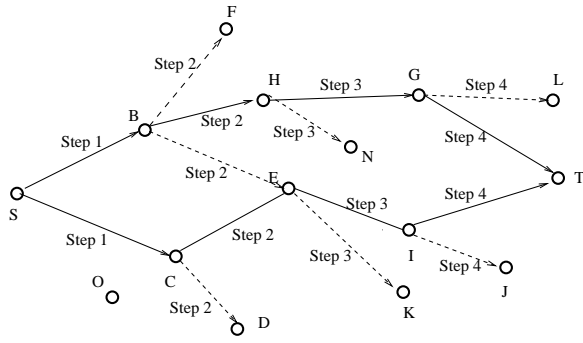


Fig. 3. MSGPR with $n = 2$.

For each MT in the original searching set, n of its neighboring MTs which are closest to the destination are found, which also form an original searching set with no more than $n \times n$ MTs (some MTs may be selected by more than one MT at the previous hops). From this original searching set, only n MTs closest to the destination are kept as the selected searching set. So n different routes starting from the source are kept. For each MT in the selected searching set, again n of its neighboring MTs which are closest to the destination are found. The procedure is repeated until the destination is included and a maximum of n different routes can be found. In the route searching process, the route diversity is kept as high as possible.

An example of this routing scheme is shown in Figure 3 with $n = 2$. The original searching sets and selected searching sets after each step are: $\langle B, C \rangle$ and $\langle B, C \rangle$; $\langle F, H, E, D \rangle$ and $\langle H, E \rangle$; $\langle G, N, I, K \rangle$ and $\langle G, I \rangle$; $\langle L, T, J \rangle$ and $\langle T \rangle$. The two selected routes are: $S \rightarrow B \rightarrow H \rightarrow G \rightarrow T$ and $S \rightarrow C \rightarrow E \rightarrow I \rightarrow T$.

To rank these n selected routes, the most important criteria considered is the packet end-to-end delay. Ignoring the propagation delay, the end-to-end delay depends on the transmission delay and the back-off delay. The transmission delay is the delay when a packet is transmitted and received. It depends on the number of hops in the route (assuming the fixed ad hoc channel bandwidth and the fixed data packet length). The back-off delay is caused by the collision during the access process and it depends on the density of MTs around the link and the corresponding traffic. To conduct routing optimization, a new metric is added—the number of reachable neighboring MTs for an MT in the route. If this number is too small, there will be less route diversity, or in the worst case, no route can be found. If the number is too large, there may be a lot of transmission collisions and a large backoff delay. The experimental value for the average backoff delay with different number of MTs using CSMA/CA can be found by simulation. The end-to-end delay for a route can then be estimated by knowing the number of hops and the number of surrounding neighboring MTs along the route. After ranking the routes, the CAMA agent sends the source MT the route with the highest rank. If the route cannot go through because of radio block, or because the route is broken due to mobility of MTs, the source MT reports to the CAMA agent. When there is no position update, a new route selected from the rest of the routes that do not include the bad

link is sent to the source MT. Otherwise, new routes have to be found again by using the routing search algorithm.

C. The Procedure for Making Routing Decisions

When an MT needs to send data to its destination, it will send a routing request to the CAMA agent through the cellular radio channel. The channel can be the random access channel, the uplink common packet channel, or a pre-assigned traffic channel in UMTS. CSMA/CD can be the random access technology for the cellular uplink access. The MT will re-send the routing request if it does not receive the routing reply after a time-out. The failure to receive a routing decision is caused mainly by collision with the hidden MTs. However, the hiding terminal problem here is not as serious as that in WLAN since the cellular radio coverage is large enough compared to the size of ad hoc network. The CAMA agent replies to the MT with a complete route including every intermediate MT through the forward access channel, the downlink shared channel, or a pre-assigned traffic channel of the cellular network. Since the positions of all the MTs are well known, the distance for each hop is also known and the transmission power of each MT can be estimated.

To further save power, MTs may “sleep” but listen to the cellular channel (e.g., the broadcast channel or the paging channel) periodically when they are not included in any active routes. When a new routing decision is made, the BS will page all the intermediate MTs on the route with the destination MT by broadcasting their IDs. These MTs will “wake up” to receive and transmit the data packets. After all the packets are received by the destination, the route will be released and all MTs on the route “sleep” again. The routing information is carried in the header of each data packet, as is in DSR [8]. The intermediate MTs read the routing decision to find their next hop, as well as the recommended transmitting power.

D. Position Update

Position update is needed when an MT moves away from its previous position. For the GPS-aided positioning routing, an MT has to send its new position to the CAMA agent through the cellular channel. The new positions are updated periodically, with a time threshold value for the update period. This value is based on the given probability of wrong routing decision caused by out-of-date position information being no more than a value p_{rt} . It mainly depends on the network traffic, i.e., how often a new route has to be determined and how often an MT is included in a new route.

It is possible that when it is time for an MT to update its position, it remains close to the position in its previous update. A new position update is not necessary since there is no change in routing topology, and position update brings signaling and operating load to the cellular network. To determine whether a position update needs to be sent, another threshold value of the distance between an MT’s updated position and its position during last update should be defined. This threshold value is based on the requirement that the probability of a one-hop link break due to the non-updated position information should be

$$d_{A'B'} = \sqrt{(d_{BB'} \cos \varphi_B - d_{AA'} \cos \varphi_A + d_{AB})^2 + (d_{BB'} \sin \varphi_B - d_{AA'} \sin \varphi_A)^2} \quad (1)$$

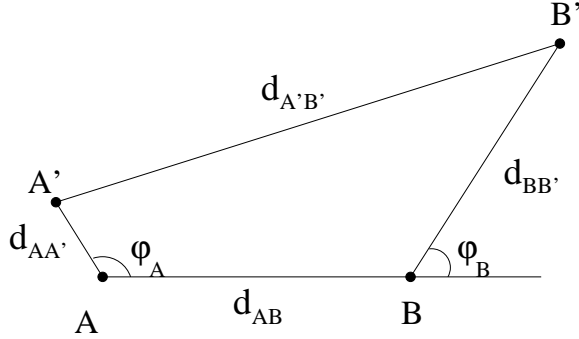


Fig. 4. An example of movements for ad hoc MTs.

no greater than $p_{\tau d}$. It should be adaptive in the networks with different MT mobility patterns.

The threshold values can be estimated mathematically. To determine the time threshold value, we assume that λ is the mean of a Poisson packet arrival to each MT, and m is the average number of hops in each link. The time interval between any two cases in which an MT has to be active in a route is approximately negative exponentially distributed with a mean of $1/(\lambda \times m)$, so that the time threshold value can be calculated by solving the equation $1 - e^{-\lambda \times m \times t_{\tau}} = p_{\tau t}$. For the distance threshold value, we assume that the original positions for two connected MTs are A and B. After a while these two MTs move to the new positions which are A' and B' respectively, as shown in Figure 4. The new distance between these two MTs, $d_{A'B'}$, is that in Eqn. 1.

Assume d_{AB} , $d_{AA'}$, $d_{BB'}$, φ_A , φ_B are independent random variables with known distributions, the probability density function (PDF) for $d_{A'B'} \leq r$ under different distance threshold values can be numerically calculated, where r is the maximum ad hoc radio coverage. From the PDF function, we can find the threshold value d_{τ} for $d_{AA'}$ and $d_{BB'}$ so that $p \leq p_{\tau d}$. A numerical result of the percentage of a link-break against different distance threshold values is shown in Figure 5.

Special updates may be needed when the radio environment for an MT changes significantly (e.g., when an MT turns a corner or goes into a building). These changes can only be measured by sending "hello" messages between MTs for reachable neighbors.

IV. SECURITY IN CAMA

Cellular networks have their own security concerns and solutions. In CAMA, our concern is for security issues related to the ad hoc network. Compared to pure ad hoc networks, achieving security in CAMA is much easier because the CAMA agent can work as a central security control point for key distributions and intrusion detections. The CAMA agent can also broadcast the information through BS whenever the network security is threatened, e.g., when an intrusion is detected or a comprised MT is found. Moreover, the positioning

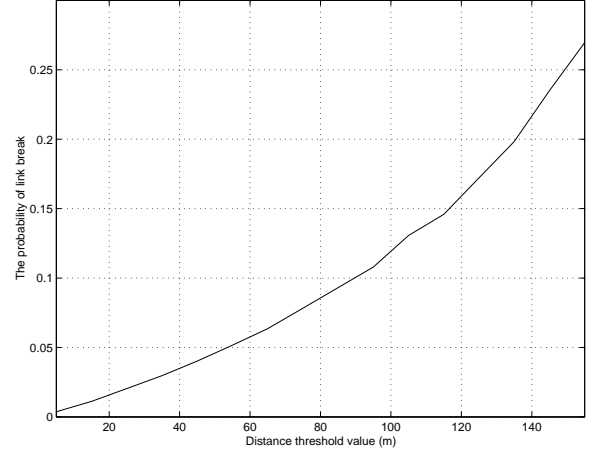


Fig. 5. Probabilities of link break vs different distance threshold values. The initial distance is Poisson distributed with a mean of 150m, and the maximum radio coverage is 250m. φ is uniformly distributed between $[0, 2\pi]$.

routing is less vulnerable than other ad hoc routing protocols such as the AODV protocol. Yet CAMA has its unique security weaknesses. In cases when the GPS signals are interfered such that MTs cannot calculate their own positions, the GPS-aided positioning routing will not work at all. This problem can only be solved by increasing the robustness of GPS technology [31] [32]. Another security weakness affecting CAMA is that the CAMA agent may be the target of attack for denial of service (DoS). This does not happen in pure ad hoc networks. However, the connection between the CAMA agent and an MT is very short, and the number of MTs in an ad hoc network normally is not very large. Therefore, it is less likely for CAMA to suffer DoS than does the wired network.

This section discusses the security problems and the proposed solutions caused by the false position information sent by MTs, by MT's Byzantine misbehavior, and by ad hoc channel jamming. It is assumed that there is no error or radio block problem in the radio channels, and the malicious MTs do not collaborate with each other.

A. Routing Security Against the Intended False Positioning Information

Due to the dynamic routing topology in an ad hoc network, an inside attack on routing information is one of the major security concerns. The routing with global positioning information makes attack on routing less possible. In the routing discovery stage, the compromised (malicious) MTs can only attack routing by sending the wrong positions. Based on this wrong information, the CAMA agent may make wrong routing decisions by including the MTs with false positions into the route. If there are relatively a large number of compromised MTs, it may cause routing problem and takes time to find the right route. This leads to increased cellular overhead and decreased ad hoc delivery ratio.

The pro-active solution for this problem is to have MTs send IDs of their reachable neighboring MTs as well. The CAMA agent can use the network association to make a judgment as to whether an MT is sending its true position or not.

The reactive solution is intrusion detection. The CAMA agent will try to find out the malicious MTs and exclude them from the network. To find out these malicious MTs, an MT sends the CAMA agent a routing failure report when it finds that its next hop actually does not exist. The report is encrypted to ensure the originality and the CAMA agent should have the public keys for all the MTs. Note that a malicious MT can also send the right position but false routing failure report claiming that it cannot find its next hop. If a malicious MT always behaves maliciously (i.e., always sends the wrong position information or send the wrong report), the malicious MTs can be eliminated easily by keeping the record of all good MTs. However, malicious MTs may act more intelligently, and can act maliciously only occasionally. In this case, by receiving each single report, the CAMA agent can only make the record of this routing failure and the link is excluded from the future routing decisions until a location update from either end of this link is received. The CAMA agent also makes question marks on both the MTs and gives them some bad credits. To encourage an MT to report a routing problem, fewer bad credits are given to MTs that report problems. After a number of reports related to the same MT are received and the accumulated bad credits for this MT reach a threshold value, the CAMA agent can make a decision that this MT is malicious and should be excluded from the network.

The decision rule can also be made on the premise that the probability of a good MT to be judged as malicious should be no more than a value, p_τ . The rule for judging malicious MTs can be defined if the ad hoc network is large enough and MTs are uniformly distributed. In this case, there is approximately an equal probability, defined as p_r , for each MT to be included in a route. p_r is also the probability that a malicious MT who sends the wrong position information to be selected in a route. For a malicious MT who sends the right position and is included in a route, it can be assumed that this malicious MT has a probability of p_f to send a false report. Then, the probability of a malicious MT that 1) sent the right position, 2) was selected in a route, and 3) sent a false report is $p_r p_f$. Since malicious MTs are not collaborative and there is no radio block, when an MT sends a routing failure report claiming it cannot find its next hop, the probability that the sender is malicious and sends the false report is $p_r p_f / (p_r + p_r p_f) = p_f / (1 + p_f)$. The probability that the sender's next hop is malicious and sends the wrong position is $p_r / (p_r + p_r p_f) = 1 / (1 + p_f)$. Note that $p_f / (1 + p_f) \leq 1 / (1 + p_f)$. It is consistent with the rule that less bad credits are given to the reporters. For an MT, if it sends the report m times and is reported as the non-existing next hop n times, the probability that it is a good MT, P is: $P = (p_f / (1 + p_f))^m (1 / (1 + p_f))^n$.

When P is smaller than p_τ , the CAMA agent can make the decision that this MT is malicious and should be eliminated from the network. This rule of judging maliciousness will not be precise in case of small sized networks or un-uniformly

distributed MT patterns. Since in those cases, some MTs (e.g., MTs close to the center of the network) may have more chances of being included in a route.

B. Security Against Byzantine Behavior

In CAMA, an MT gets to know the route from the CAMA agent and this route is carried in the header of the data packet. The MTs on the route can read the routing decision from the packet header, thereby knowing where the next hop is. To prevent the routing information from being changed by the intermediate malicious MTs, the information is encrypted using the source MT's secret key. The CAMA agent sends the source MT's public key to the intermediate MTs when it pages them to wake up. The intermediate MTs can read the routing information, but cannot change it. It is possible that an intermediate compromised MT interrupts the routing information such that the MT on its next hop cannot read it. In this case, the next hop MT will report to the CAMA agent through the cellular channel. The rule for judging a malicious MT is the same as that used in detecting MTs who send the false position information.

The intermediate compromised MTs can also interrupt the data. Watch Dog scheme in [30] can be used to avoid this attack. The disadvantage of "Watch dog" is discussed before. If the watch dog scheme is not used, the corruption of data will not be found until the destination MT tries to decrypt it. This is because data should be encrypted by a secret key only known to the source and destination MTs. Without any central control point, to find out questionable MT is difficult. The source may have to ask every intermediate MT to send a copy of its received data packet to match with the original one. In CAMA, with the help of CAMA agent, the bad link can be found more easily. There are two ways to detect such a bad link: the downlink data match and the uplink data match.

In the downlink data match, the CAMA agent broadcasts the Hash code for the original packet to all the intermediate MTs. These MTs can compare their own Hash codes with the right one. MTs then send a message confirming to the CAMA agent whether or not they received the correct data packet. This message may contain only one bit of information (0 or 1) and can be piggy-backed in some other uplink messages (e.g., the position update message). Based on the information it collects, the CAMA agent can find questionable MTs. The downlink data match method occupies less cellular radio bandwidth but does not work when there are more than one malicious MT in the route since malicious MTs may intend to send wrong messages.

In the uplink data match, the intermediate MTs send the CAMA agent the Hash codes generated from the data they received and the CAMA agent makes a comparison to find out which intermediate MT received the corrupted data packet. Note that a malicious MT can only send a false message when it receives a good data packet, but it sends a wrong Hash code. It is easy to make the decision rule for the uplink data match, which is:

From the MTs that send the right Hash code, the one closest to the destination and its next hop (this next hop MT sent a

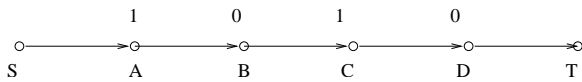


Fig. 6. Example of Hash code comparison.

wrong Hash code) are questionable, and the MTs between it and the source that send wrong Hash codes are malicious.

The uplink and downlink data match are compared given the example Hash code comparison shown in Figure 6. In Figure 6, a source S sends a data packet to the destination T through intermediate MTs A, B, C, and D. T receives a corrupted data packet so a downlink data match is used. 1 is used when an MT claims that it received a good data packet and 0 is used when an MT claims it received a corrupted data packet. For the downlink match, it is difficult to make a decision since all A, B, C, D are questionable. With the uplink match, we know B is malicious and C, D are questionable. The uplink data match simplifies the judging rule, but it needs more uplink cellular bandwidth since all the intermediate MTs have to send their Hash codes to the CAMA agent separately.

C. Anti-Jamming

One critical weakness for current ad hoc routing is in its MAC layer, where a CSMA/CA random access technique is used. An outside attacker can simply send strong noise to jam the ad hoc wireless channel. All MTs nearby will detect that the channel is busy and based on CSMA/CA rule, they will back-off. If the attacker keeps on sending the strong but meaningless signal, all the MTs around it can not send data at all.

If there is only one channel in the ad hoc network, the problem cannot be solved. However, if more than one channel can be used, and there is good medium access control scheme for ad hoc networks with multiple channels, the MTs can pick another channel to avoid the channel jamming. The problem is: how does the receiver know it should switch to another channel? Additionally, sometimes it is difficult for MTs to tell whether the noise comes from the attacker or it is just the data sent by its neighboring MTs. In CAMA, the CAMA agent makes the routing decisions and keeps all the routing information. After the CAMA agent receives a report that there is a possible jamming, it may check its routing record to find out whether it is a real jamming or it is because of high traffic density. The BS may broadcast warning of the jamming so the MTs can switch channels. MT pairs then exchange messages through cellular channels to decide exactly when to switch, and which channel to switch to. MT pairs can jump among the channels to avoid future jamming. A good jumping sequence can be used to keep the attacker from chasing the MTs.

There is also a possibility that an attacker may jam the cellular channel, but it is difficult for the attacker to jam both the cellular channel and the ad hoc channel at the same time. In a case when the attacker jams all the ad hoc channels, data can still be transmitted through the cellular channel or, at least the CAMA agent can inform MTs to give up accessing attempts.

V. IMPORTANT SIMULATION RESULTS

A. General Simulation Model

The most recent version (2.26) of the network simulator ns2 is used for the experimental study. We simulate an ad hoc network with 100 MTs residing in an area of $1000m \times 1000m$. Each MT moves within the area, with a random direction and a random velocity uniformly distributed between 0 and a maximum value. Without any specification, this maximum value is $3m/s$, the speed for pedestrian users. The ad hoc channel has a fixed data rate of $1Mb/s$. The wireless interface works like the $914 MHz$ Lucent WaveLAN, with a nominal radio range of $250m$. MSGPR (multi-selection greedy positioning routing) under CAMA environment is compared with two other ad hoc routing protocols, AODV and DSR. The searching set for MSGPR is set large enough so that the best route can always be found. We assume that position updates and routing requests can always be sent successfully to the CAMA agent at their first attempts. In this work, the case that MTs send their associations with neighboring MTs is not included.

B. Delivery ratio and cellular overhead

The delivery ratio (goodput) and the corresponding routing overhead for MSGPR, AODV, and DSR are shown in Figure 7 and Figure 8. The routing overhead for MSGPR includes the routing requests, routing replies, and position updates going through the cellular radio channel. It is shown that MSGPR has a much better delivery ratio than AODV and DSR. The routing overhead in MSGPR is also much lower. When the number of active links increases, the delivery ratio for MSGPR decreases, as is the case with AODV and DSR. This is due to the increased collision in the MAC layer. The overhead for MSGPR increases marginally when the number of active links increase due to the increasing number of routing requests and replies.

The routing overhead in MSGPR is also a cost in the cellular network. The gain when using MSGPR over the AODV and DSR is shown in Figure 9. The gain in the ad hoc networks (the number of additional bytes delivered successfully than would be in AODV and DSR) is approximately 10 times as large as the cellular overhead at the medium network load and high network load. For networks with low load, the gain is even larger. For commercial wireless services, it is worth using CAMA if a byte in a cellular network is no more than 10 times the value of a byte in an ad hoc network.

C. Maximum Hop Distance

In greedy positioning routing, an MT always tries to find the MT closest to the destination as its next hop. This reduces the average number of hops for links and improves delivery ratio. However, if the maximum hop distance is too large (e.g., as large as the maximum radio coverage), the link may break quickly due to the MT mobility and a new route may have to be found. An optimum value for the maximum hop distance needs to be found. Note that the actual hop distance is smaller than the maximum hop distance.

The packet delivery ratio using different maximum hop distance in MSGPR is shown in Figure 10. The delivery ratio

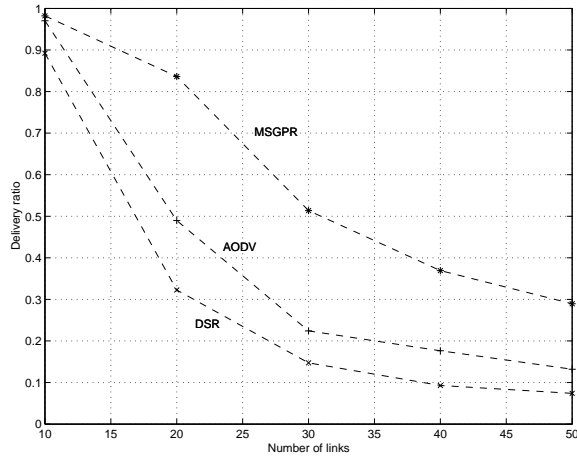


Fig. 7. Delivery ratio comparison among MSGPR, AODV, and DSR.

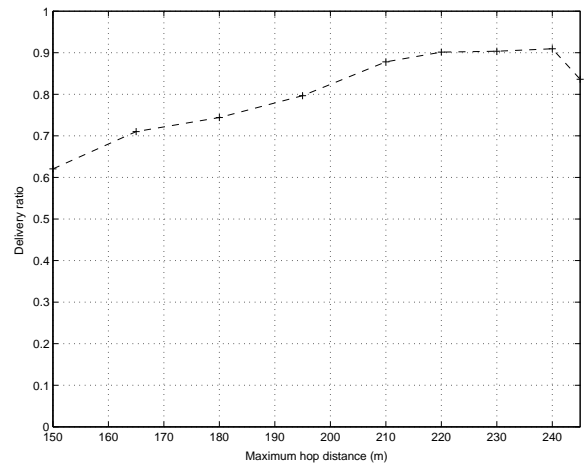


Fig. 10. Delivery ratio vs maximum hop distance.

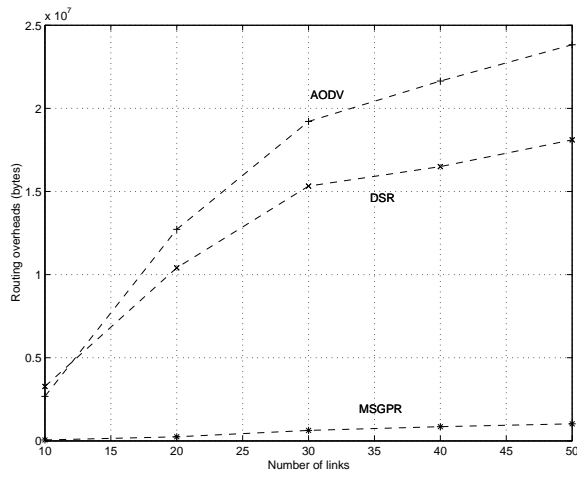


Fig. 8. Routing overhead comparison among MSGPR, AODV, and DSR.

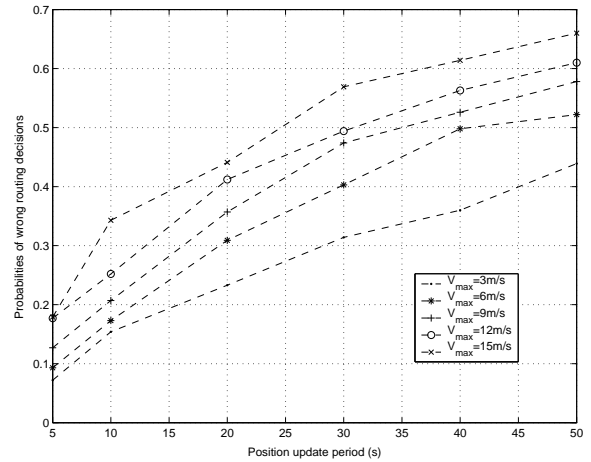


Fig. 11. Probabilities of wrong routing decisions vs position update period.

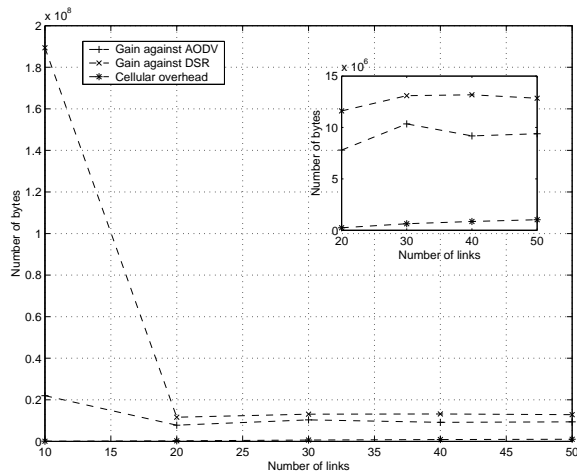


Fig. 9. Gains when using CAMA.

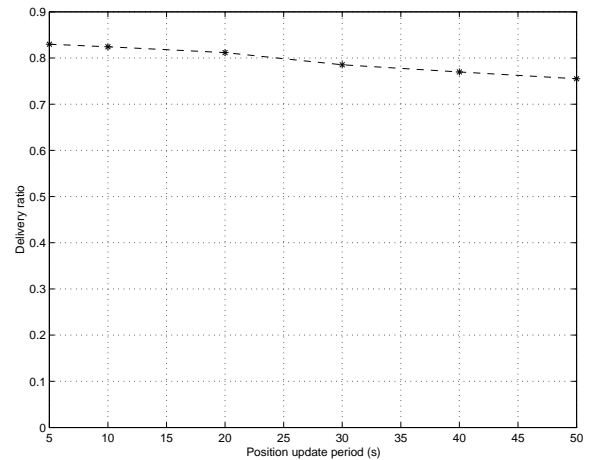


Fig. 12. Delivery ratio vs position update period.

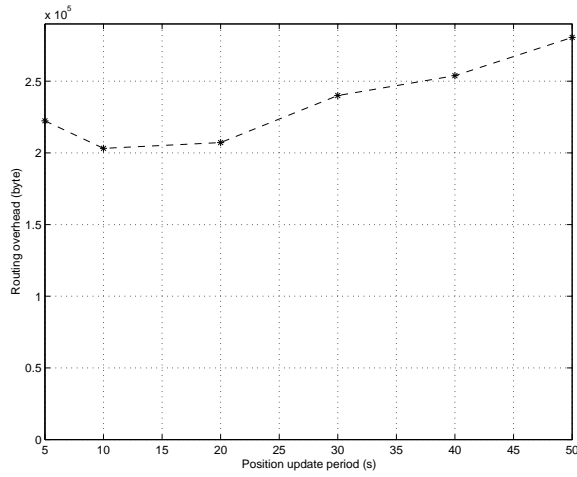


Fig. 13. Cellular overheads vs position update period.

increases when the maximum hop distance increases. When the maximum hop distance approaches the maximum radio coverage radius, the delivery ratio drops. Simulation results show that the optimum value is in the range of $210m - 240m$.

D. Position Update Period

Figure 11 shows the probability of wrong routing decisions when using different position update time periods. The wrong routing decisions include both the routes that do not work at all (because some links actually do not exist), as well as the routes that are not the optimum ones. The longer the period, the greater the likelihood of a routing decision being wrong because it may be based on the past position information, which may not be accurate anymore. The probability increases when the maximum speed increases, since it is more probable that an MT with a higher speed moves further away from its previous position, and the link based on this MT's previous position is more likely to fail.

Figure 12 shows the delivery ratio for different position update periods. A medium load (20 active links) is considered for the ad hoc network. The delivery ratio decreases when the position update period increases. This is due to the fact that when the position update period increases, there is a greater probability of a wrong routing decision being made based on past position information. In Figure 13, the corresponding cellular load (routing overhead) is shown. When the position update period increases, at the beginning, the overall cellular overhead decreases. The reason is that the decreased overhead for the position update compensates for the increased routing requests and replies. However, when the position update period reaches a certain value, the increased overhead of routing requests and replies is more dominant, so the overall cellular overhead increases.

E. Robustness for GPS-Aided Routing Protocol

Since the attack on position information is unique to the proposed architecture, in this simulation, the robustness of GPS-aided positioning routing against the attack of false position reports is tested. The network being tested has a size

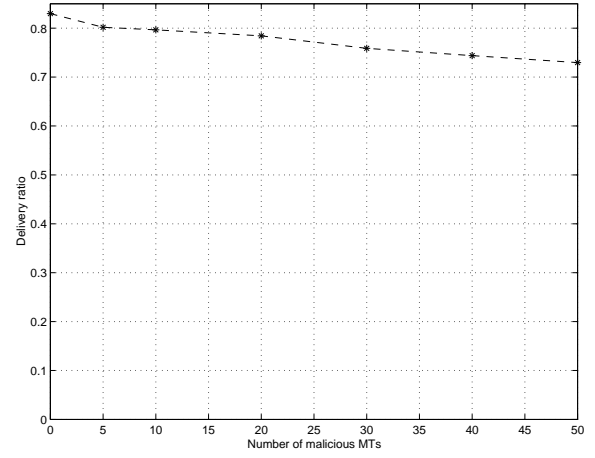


Fig. 14. Delivery ratio vs Numbers of malicious MTs.

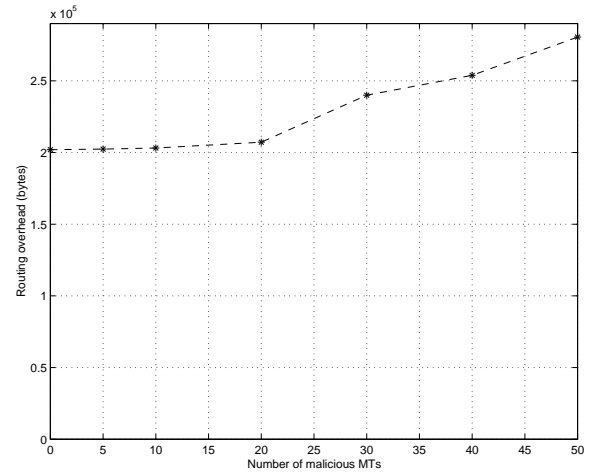


Fig. 15. Cellular overhead vs number of malicious MTs.

of 100 normal MTs and 20 active connections. An increasing number of malicious MTs join the network and send wrong position information.

Figure 14 shows the relationship between delivery ratio and different numbers of malicious MTs. The delivery ratio decreases only marginally. This is because the routing scheme has a quick, self correcting ability, i.e., whenever a bad route caused by the false position information is found, a new route can be decided very quickly. However, this increases the routing overhead because more routing requests and replies are needed. The routing overhead is shown in Figure 15. Such an attack causes more damage to the network when there are a large number (i.e., 20) of malicious MTs. The detection method then needs to be applied.

F. Simulation summary

The following is the summarized simulation results:

- MSGPR in the proposed architecture greatly improves delivery ratio in the ad hoc with little cellular overhead.
- When making routing decision, MSGPR should use the longest hop distance. Very little margin is needed for the maximum hop distance and the maximum radio coverage.

- Long position update period may decrease the network delivery ratio and increase the cellular overhead. The effect is not significant because of the ability of quick routing re-selection in the proposed routing scheme.
- MSGPR is robust against the attack of false position information. Intrusion detection is needed only when there are large numbers of malicious MTs.

VI. CONCLUSIONS

A novel network architecture—the cellular-aided mobile ad hoc network (CAMA)—is proposed. In this architecture, a cellular network is overlaid on the ad hoc network and a mobile ad hoc agent (CAMA agent) in the cellular network will manage the control signaling for the ad hoc network. Data traffic remains in the ad hoc network. When applying the architecture, the ad hoc network performance can be greatly improved with limited cellular overhead. This architecture is also less vulnerable than a pure ad hoc network because of the availability of a central control point. The possible attacks on the architecture and the proposed solutions are addressed.

ACKNOWLEDGMENT

This research is supported by CERIAS, Motorola Inc., NSF grants CCR-0001788 and ANI-0219110, and CISCO URP grant. We also thank Dr. Dongyan Xu for his help and support.

REFERENCES

- [1] Navstar gps operation. *Web site at <http://tycho.usno.navy.mil/gpsinfo.html>.*
- [2] J. Ala-Laurila, J. Mikkonen, and J. Rennemaa. Ieee 802.11: Wireless local area networks. *IEEE Communications Magazine*, Sept 1997.
- [3] P. Albers, O. Camp, J.-M. Percher, B. Jouga, L. Me, and R. Puttini. Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches. *Web site at www.supelec-rennes.fr/ren/perso/bjouga/documents/.*
- [4] N. Asokan and P. Ginzboorg. Key agreement in ad-hoc network. *Web site at www.cs.umd.edu/sengcy/classes/818y.*
- [5] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. An on-demand secure routing protocol resilient to byzantine failures. In *Proceedings of ACM Workshop on Wireless Security*, pages 21–30, 2002.
- [6] J. Binkley and W. Trost. Authenticated ad hoc routing at the link layer for mobile systems. *Wireless Networks*, 7, 2001.
- [7] L. Blazevic, L. Buttyan, S. Giordano, J.-P. Hubaux, and J.-Y. L. Boudec. Self-organization in mobile ad hoc networks: The approach of terminodes. *IEEE Personal Communications*, June 2000.
- [8] J. Broch, D. B. Johnson, and D. A. Maltz. The dynamic source routing protocol for mobile ad hoc networks. *IETF Internet Draft*, 1998.
- [9] S. Buchegger and J.-V. L. Boudec. Performance analysis of the confidnet protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks). In *Proceedings of Mobicom'2002*, 2002.
- [10] B. Carp and H. T. Kung. Gpsr: Greedy perimeters stateless routing for wireless network. In *Proceedings of ACM/IEEE Mobicom*, pages 243–254, 2000.
- [11] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai. Ieee 802.11: Wireless local area networks. *IEEE Communications Magazine*, Sept 1997.
- [12] E. Dahlman, B. Gudmundson, M. Nilsson, and J. Skold. Umts/imt-2000 based on wideband cdma. *IEEE Communications Magazine*, Sept 1998.
- [13] Y. Desmedt. Threshold cryptography. *European Transactions on Telecommunications*, 5(4), July-Aug., 1994.
- [14] A. Doskow. Signaling system 7 (ss7). *Web site at <http://www.iec.org/online/tutorials/ss7/index.html>.*
- [15] A. Guntsch, M. Ibnkahla, G. Losquadro, M. Mazzella, D. Roviras, and A. Timm. Eu's r & d activities on third-generation mobile satellite system (s-umts). *IEEE Communications Magazine*, Feb 1998.
- [16] M. Hietalahti. Key establishment in ad-hoc networks. *Web site at www.camars.kaist.ac.kr/hyoon/courses/cs710_2002_fall/2002cas/security/papers.*
- [17] H. Hsieh and R. Sivakumar. On using the ad-hoc network model in cellular packet data networks. In *IEEE proceedings of Mobihoc*, 2002.
- [18] J.-P. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *Proceedings of MOBIHOC 2001*, pages 146–155, 2001.
- [19] R. Jain and R. Sengupta. Geographic routing using partial information for wireless ad hoc networks. *IEEE Personal Communications*, Feb 2001.
- [20] H. Kaaranen, A. Ahtianen, L. Laitinen, S. Naghian, and V. Niemi. *UMTS Networks: Architecture, Mobility and Services*. John Wiley and Sons, 2001.
- [21] V. Karpjoki. Security in ad hoc networks. *Web site at www.tcm.hut.fi/Opinnot/Tik-110.501/2000/papers.*
- [22] Y. Ko and N. H. Vaidya. Location-aided routing in mobile ad hoc network. In *Proceedings of ACM/IEEE Mobicom*, pages 66–75, 1998.
- [23] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. In *Proceedings of IEEE International Conference on Network Protocols*, 2001.
- [24] F. Kuhn, R. Wattenhofer, and A. Zollinger. Asymptotically optimal geometric mobile ad-hoc routing. In *Proceedings of ACM Dial-M*, pages 24–33, 2002.
- [25] J. Li, J. Jannotti, D. D. Couto, D. R. Karger, and R. Morris. A scalable location services for geographic ad hoc routing. In *Proceedings of ACM/IEEE Mobicom*, pages 120–130, 2000.
- [26] W. Liao, Y. Tseng, and J. Sheu. Grid: A fully location-aware routing protocols for mobile ad hoc networks. In *Proceedings of IEEE HICSS*, Jan, 2000.
- [27] C. R. Lin and M. Gerla. Adaptive clustering for mobile wireless networks. *IEEE Journal on Selected Areas in Communications*, 15, Sept., 1997.
- [28] X. Lin, M. Lakshdisi, and I. Stojmenovic. Location based localized alternate, disjoint, multi-path and component routing algorithm for wireless networks. In *Proceedings of ACM/IEEE Mobhoc*, Oct., 2001.
- [29] Y. Lu and B. Bhargava. Achieving scalability and flexibility: A new architecture for wireless network. In *Proceedings of Conference on Internet Computing 2001*, 2001.
- [30] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile wireless networks. In *Proceedings of Mobicom'2000*, 2000.
- [31] W. Myrick, M. D. Zoltowski, and J. S. Goldstein. Low-sample performance of reduced-rank power minimization based jammer suppression for gps. In *IEEE Sixth International Symposium on Spread Spectrum Techniques & Applications (ISSSTA 2000)*, Aug 2000.
- [32] W. Myrick, M. D. Zoltowski, and J. S. Goldstein. Adaptive anti-jam reduced-rank space-time preprocessor algorithms for gps. In *Institute of Navigation (ION) Conference*, Sept 2000.
- [33] K. Pahlavan, P. Krishnamurthy, A. Hatami, M. Ylianttila, J. P. Makela, R. Pichna, and J. Vallstron. Handoff in hybrid mobile data networks. *IEEE Personal Communications*, Apr 2000.
- [34] P. Papadimitratos and Z. J. Hass. Secure routing for mobile ad hoc networks. In *Proceedings of CNDS 2002*, 2002.
- [35] B. Parkinson and S. Gilbert. Navstar: global positioning system - ten years later. In *Proceedings of IEEE*, pages 1177–1186, 1983.
- [36] C. A. Perkins, E. M. Royer, and S. R. Das. Ad-hoc on-demand distance vector routing. *IETF Internet Draft of AODV, version 10*.
- [37] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing for mobile computers. *Computer Communication Review*, Oct 1994.
- [38] A. K. Salkintzis, C. Fors, and R. Pazhyannur. Wlan-gprs integration for next-generation mobile data networks. *IEEE Communications Magazine*, Oct 2002.
- [39] S. Chakrabarti and A. Mishra. Qos issues in ad hoc wireless networks. *IEEE Personal Communication Magazine*, pages 142–148, Feb 2001.
- [40] C. Schwingenschlogl and M.-P. Horn. Building blocks for secure communication in ad-hoc networks. In *Proceedings of European Wireless 2002*, 2002.
- [41] A. Sumukic. Umts universal mobile telecommunications system: Development of standards for the third generation. *IEEE Transactions on Vehicular Technology*, Nov 1998.
- [42] P. Taaghola, B. G. Evans, R. D. Gaudenz, G. Gallinaro, J. Lee, and C. Kang. Satellite umts/imt2000 w-cdma air interface. *IEEE Communications Magazine*, Sept 1999.
- [43] C. K. Toh. Associativity-based routing for ad-hoc mobile networks. *IEEE Wireless Personal Communications Magazine*, 4(2), Mar 1997.
- [44] W. Wang and B. Bhargava. On vulnerability and protection of ad hoc on-demand distance vector protocol. *Accepted to appear in proceedings of International Conference on Telecommunication (ICT)*, 2003.

- [45] H. Wu, C. Qiao, S. De, and O. Tonguz. An integrated cellular and ad hoc relaying system: icar. *IEEE Journal on Selected Area in Communications*, 19(10):2105–2115, Oct. 2001.
- [46] X. Wu, B. Mukherjee, and G.-H. Chan. Maca: An efficient channel allocation scheme in cellular network. In *IEEE proceedings of Globcom*, volume 144, 2000.
- [47] M. Ylianttila, M. Pande, J. Makela, and P. Mahonen. Optimization scheme for mobile users performing vertical handoffs between ieee 802.11 and gprs/edge networks. In *IEEE proceedings of Global Telecommunications Conference*, volume 6, 2001.
- [48] M. G. Zapata and N. Asokan. Securing ad hoc routing protocols. In *Proceedings of ACM Workshop on Wireless Security*, pages 1–10, 2002.
- [49] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of Mobicom'2000*, 2000.
- [50] Z. Zhou and Z. Hass. Secure ad hoc networks. *IEEE Networks*, 13(6):24–30, 1999.