SECURE COMMUNICATIONS OVER HYBRID MILITARY NETWORKS

Vamsi Paruchuri
University of Central Arkansas
Conway, AR, USA
vparuchuri@uca.edu

Arjan Durresi
Purdue School of Science, IUPUI
Indianapolis, IN, USA
durresi@cs.iupui.edu

Sriram Chellappan
Missouri University of Science and Technology Rolla, MO, USA
chellaps@mst.edu

ABSTRACT

Stealthiness can be described as a disposition to be sly and to do things surreptitiously. This paper presents a new architecture for flexible and secure networking in battlefields that enables stealthy and covert communication in the presence of node mobility. Our architecture is based on the combination of optical (fiber) and wireless links. Our objective is to be able to carry on undeterred communication without the attack/eavesdropping nodes being able to detect the presence of any communication. This objective is not only crucial for successful completion of the operation, but also for the safety of our mobile nodes, by not giving out their locations.

We combine the advantages of optical links, such as high bandwidth, low delays, low error rates, good security, with the advantages of wireless links, such as mobility and flexibility, along with directional antennas for communication. From security point of view, we also assume presence of red zones, which are the ones controlled by the adversary or where the adversary can trace wireless activities.

INTRODUCTION

Wireless communications offer an attractive option for many military, commercial as well as personal communication needs because of flexibility, cost effectiveness, and mobility support. However, for several security reasons, the devices prefer to minimize communication wirelessly. For example, wireless communication is more susceptible to jamming attacks and also might leak critical information such as location of communicating nodes. Even if strong encryption techniques could be used to hide this information, it is infeasible to hide the location of the transmitting nodes. Thus, the broadcast nature of these wireless networks might jeopardize the lives of the mobile nodes and even the objective of the mission, since any enemy/eavesdropping node can detect ongoing communication and could sense the presence of troops. The eavesdropping nodes might even be able to compute the locations of the communicating nodes and thus endanger their lives.

978-1-4244-2677-5/08/$25.00 ©2008 IEEE

On the other hand, optical networks can offer high transmission rates that can accommodate broadband needs, provide error-free transmissions and most importantly they are immune to eavesdropping and jamming attacks. But, they do not provide the flexibility and mobility support that wireless networks offer.

Often, one might not be able to control the extent of optical coverage in a given network area. This challenge arises because most of the times, one might be utilizing the existing optical links. Deploying new optical links might not be feasible for practical reasons; cost issues; the mission might be temporary, the need might be immediate and there might not be enough time to deploy a complete optical network.

This paper presents a new architecture for flexible and secure networking in battlefields for enabling covert communication. Our architecture is based on the combination of optical and wireless links. This advantage of fiber optical links was demonstrated during recent conflicts in the Middle East.

Our objective is to be able to carry on undeterred communication without the attack/eavesdropping nodes being able to detect the presence of any communication. To quantify this, we define a new metric in this paper called *stealthiness* – that is the probability that an on-going communication among benign nodes in the network cannot be detected by the adversary.

We propose hybrid network architecture and a new Stealthy Routing Protocol (SRP) to exploit the optical links. The proposed routing protocol intelligently selects appropriate routes to maximize *stealthiness* and minimize the probability of the communication being detected by any malicious nodes present in the network. Our architecture also considers communication via directional antennas, which are available today in numerous forms and sophistications. Further, we assume both passive and active malicious adversaries; a passive adversary can only detect and perceive ongoing communication, while an active adver-

sary can compromise a node and use the node to actively participate in routing or other network operations. Through extensive simulation and analysis, we show that exploiting optical links, along with directional antenna based wireless communication could drastically improve the *stealthiness* of the network.

From security point of view, we assume presence of red zones, which are the ones controlled by the adversary or where the adversary can trace wireless activities. It is crucial that communication range and routes be selected so as to not to overlap these regions.

The rest of this paper is organized as follows: we first present related work with respect to both wireless networks and optical networks. Then, we present our network architecture. We then present and analyze the proposed Stealthy Routing Protocol and finally, we conclude the paper with some final remarks.

RELATED WORK

Over the past few years, research into ad hoc networks has yielded considerable advances, notably in the areas of new routing and medium access techniques. Wireless communication networks have also been deployed in disasters and are currently considered the most reliable and flexible communications means for disastrous events, owing to their flexibility and mobility support [1,2].

Directional antennas offer tremendous potential for improving the performance of ad hoc networks. Directional antennas have a number of advantages over omnidirectional antennas in ad hoc networking. By focusing energy only in the intended direction, directional antennas can increase the potential for spatial reuse and can provide longer transmission and reception ranges for the same amount of power. A number of protocols for wireless ad hoc networks with directional antennas have been proposed and studied. For instance see [3,4,5,6], where the approximate directional antenna pattern is considered as a circular sector with radius r and angle θ. Therefore, the area where the transmission could be detected is:

$$A(r,\theta) = \frac{\theta}{2} r^2$$

Optical networking, with its almost unlimited bandwidth, is also attractive for several other reasons - most important being they are immune to eavesdropping and jamming attacks. Several works have tried to combine wireless and optical networking technologies especially to solve the "last mile problem" [7, 8, 9, 10] but not for security reasons.

Previous research on data communication has not exploited hybrid device capabilities for security purposes. They either consider pure wireless networks or optical networks to evaluate security. Our novel architecture, described next, is tailored to deal with the unique constraints and event dynamics of military networks and achieve covert communications without degradation in network connectivity or performance.

NETWORK ARCHITECTURE

We assume a *hybrid* network which consists of both optical links and wireless links as shown in Figure 1. We specify the different components of the network as follows:

- Optical links with the end points equipped with a transceiver and we denote them as Access Points (APs); the optical links can offer high transmission rates that can accommodate broadband needs and provide error-free transmissions. However, APs are fixed and hence are immobile. APs are assumed to form an interconnected (backbone) with each other via optical links.
- Wireless mobile nodes equipped with power controlled steered directional antenna systems; we assume that the wireless mobile nodes are equipped with GPS or similar devices and thus, are aware of their location with reasonable accuracy. Because of mission oriented nature of these networks, we think this is a reasonable assumption.
- Red zones consisting of enemy nodes whose objective is to track and observe the actions/movement of mobile wireless nodes; their objective might be more intense and might involve actions like jamming and destroy. Thus, the objective of the communication protocol is to carry on communication without being detected. Note that those zones that are suspected of being under surveillance by an enemy agent are the red zones. It is also possible that some other un-suspected zones can also be 'un-known' red zones if they are under surveillance by an adversary.

STEALTHY ROUTING PROTOCOL

In this section we present the architecture for enabling undeterred and undetectable communication among the nodes. The complete protocol is described below.

1. Network Setup

Each wireless mobile node (MN) in the network is given the information regarding every Access Point in the network. The information most importantly includes the Public Key of the AP and the location of the AP. Since the number of APs is assumed to be limited and as the information is not dynamic, this imposes negligible bandwidth /

communication overhead. Further, each AP is provided the access to the Public Keys of all the mobile nodes (PK_{N-i}). Well known authentication schemes based on asymmetric encryption can be used to protect the network against active attacks like false message injection, selective dropping, sybil, breaking confidentiality etc.

2. Network Updates

Every MN in the network periodically sends an update regarding its location to the nearest AP. If a MN is aware of its destination or the path/direction it is going to further move on, the MN includes this information in the update[1].

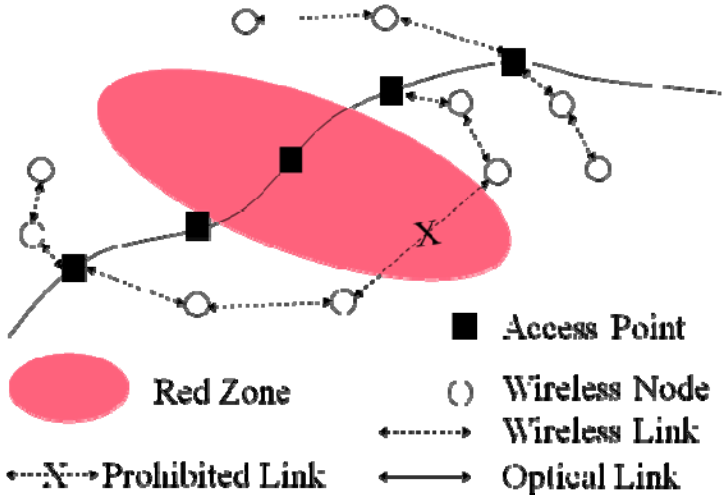


Figure 1: The network consists of wireless mobile nodes and Access Points for them to communicate via optical links. Some enemy nodes might be present in the network.

Since, the MN knows its own location, it could compute the nearest AP from the list it maintains and then could compute the direction and transmission power level needed to reach the AP. Thus, by transmitting with just enough energy and in only one direction, the MN can minimize the probability of being detected by enemy nodes.

Each AP periodically aggregates the location information of all the nodes to which it is the nearest AP and distributes the information to the rest of the APs. Since, optical links offer high bandwidths, these updates would not affect the performance of the network.

Further, to avoid all MNs from sending update messages simultaneously, the period start times are randomly assigned to each MN. This would alleviate the update message implosion at the APs. Moreover, the period intervals could be constant for all the MNs or they might be different. If they are different, the interval would be dependant not only on the speed of the MN but also other factors such as importance of the mission, security level of the region and others. For simplicity, in this paper, we assume a constant period interval for all nodes.

[1] Since, we consider a mission oriented scenario, we assume the MNs often know where they are going and hence, this information might be exploited for routing purposes.

3. Routing Decision: One-hop or Multiple Hops

Whenever a MN has to communicate to an AP or vice versa, a decision has to be made whether the MN (or the AP) has to send the packet directly to the AP (or the MN) or use intermediate nodes to relay the packet. In the presence of directional transmission, relaying the packet through intermediate node not only saves power but also, more importantly, decreases the probability of being detected.

Whenever a wireless MN is involved in communication, an AP chooses a route so as to minimize the detection probability. This routing problem could be easily solved similar to shortest path problem – construct a graph with the cost of the edge between to wireless nodes set to square the distance between them and then, compute the route with the shortest cost (since the probability of being detected depends on the area of transmission). It could be easily proven that this is the optimal path to minimize the detection probability.

4. Stealthy Communication

We categorize the communication between the nodes into four categories. Here, we describe each category and explain the routing process for each. For all kinds of communication, the messages carry a Message Authentication Code (MAC) so that the destination can verify that the message was indeed sent by the sender and the messages are encrypted using the destination's public key so that only the destination can read the message thus preserving the secrecy.

a. *AP-to-AP:* Since these messages are from one AP to another, these could be completely routed across optical links and hence are very secure and undetectable by enemy nodes.

b. *MN-to-AP:* In this scenario, a MN sends a packet to an AP. For this purpose, the MN computes the nearest AP based on its location and the location table of the APs; then it transmits the message to the nearest AP. In scenarios, where multiple packets has to be sent by the MN, the AP computes the optimal path that minimizes the probability of transmission detection (as described in previous section) and sends this information to the MN. The MN then uses this path for further communication.

c. *AP-to-MN:* This scenario is similar to the above scenario. The AP first computes the optimal path and establishes a path to the MN through that path and further communication takes place through this path.

d. *MN-to-MN:* This scenario could further be divided into two scenarios

- The simplest scenario is when the MNs have different APs as their nearest APs. Then, the nearest APs first establish optimal paths between themselves and the corresponding MNs and then MNs communicate through the APs. This scenario could be seen as a combination of above two scenarios.
- Both MNs have same AP as their nearest AP. In this scenario, the AP first computes the optimal path between the MNs and forwards this information to the MNs. Then the MNs establish a path via this path and initiate communication along this path.

5. Routing in presence of Red Zones

In hostile scenarios, one can envision presence of enemy troops in some areas inside the network coverage area, as shown in Figure 1. The routing protocol has to ensure that the locations of transmitting nodes are not disclosed to the enemy.

Our Stealthy Routing Protocol (SRP) chooses routes around these Red Zones so as to minimize the probability of detection. Once any information regarding a Red Zone is collected at an AP, the AP first broadcasts this information to all other APs. Then, each AP communicates this information to each MN through direct communication.

ANALYZING THE STEALTHINESS

In this section, we illustrate the performance analysis of the proposed SRP for a simple network with omnidirectional wireless radiation patterns. For simplicity we assume a square network of length *L*. The analysis presented can be easily extended to other networks. Further, for simplicity, where required, we use first order approximations.

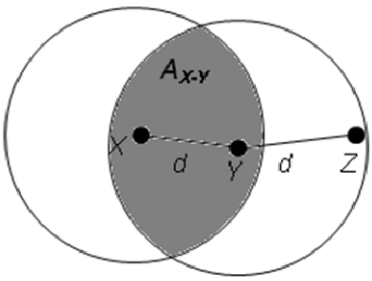


Figure 2. Area of overlap for computing the probability of detection

1. Stealthiness of a omnidirectional wireless path

Assuming omnidirectional propagation, we compute the stealthiness of a transmission in presence of an adversary. Initially, assume the presence of only one enemy node that can be arbitrarily located in the network and whose location is not known. If A is the whole network area, then the probability of a transmission being detected (P_D) could be approximated as follows:

$$P_D = \frac{A_c}{A}$$

Now consider a two-hop communication between nodes X and Z through an intermediate node Y, see Figure 2. A_c is the area covered by one transmission. However, when two neighboring nodes transmit, to compute the area covered by both transmissions need to be considered. Thus, for this scenario, the probability that the communication between X and Z is overheard is

$$P_D^{X-Z} = 1 - \left(1 - \frac{Ac}{A}\right)\left(1 - \frac{Ac - A_{X-Y}}{A}\right)$$

The first term in the compound term in the RHS is the probability that the transmission by node X is not detected and the second corresponds to the conditional probability that the probability by Y is not detected given that transmission by X is not detected.

To generalize, the probability that a communication along a *h*-hop path is detected in presence of α adversary nodes can be computed as follows:

$$P_D^h = 1 - \left(1 - \frac{Ac}{A}\right)^{\alpha}\left(1 - \frac{Ac - A_{avg\_overlap}}{A}\right)^{(h-1)*\alpha} \quad (1)$$

Finally, given the distance between two neighbor nodes is *d* and the transmission range is R, the area of overlap can be computed as

$$A_{overlap} = 2R^2\left(\frac{d}{2R}\right) - \frac{d}{2}\sqrt{(2R-d)(2R+d)}$$

The stealthiness is the probability of communication being undetected and can simply be computed as

$$S = 1 - P_D^h \quad (2)$$

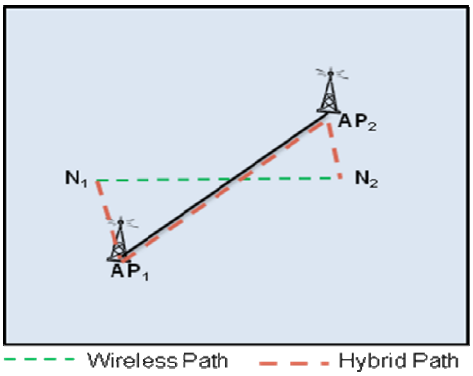


Figure 3. Choosing a path: pure wireless or hybrid?

2. Stealthiness of a wireless network

Consider a square network of length L. Average distance between a random source-destination pair could be considered to be equivalent to the average distance (d) between two points randomly selected within a square of length L. The average distance between two points picked at random from the interior of a unit square is the $n = 2$ case of hypercube line picking [11], i.e.,

$$d = \int_0^1\int_0^1\int_0^1\int_0^1 \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}\, dx_1 dx_2 dy_1 dy_2$$

$$\text{i.e., } d = \frac{1}{15}\left[\sqrt{2} + 2 + 5\ln\left(1+\sqrt{2}\right)\right] \approx 0.5214 \qquad (3)$$

For a square network of length L, the distance can be computed by simply scaling the above number i.e., the average distance is 0.5214*L.

The average number of hops for a path (h) between a source-destination pair can be derived from the Euclidean distance (d) between the two nodes [12]. For lack of space, we do not repeat the results and we refer the interested reader to [12]. Thus, using Equations (1), (2) and (3), one can compute the stealthiness of a wireless path.

3. Stealthiness of a hybrid network

Consider a network a shown in Figure 3. A node chooses a path that maximizes the stealthiness. In other words, the smaller the number of wireless hops, the larger the *stealthiness*. Thus, for source-destination pair N_1-N_2, the choice is between a pure wireless path N_1-N_2 or a hybrid path N_1-AP_1-AP_2-N_2 (assuming AP_1 is closer to N_1 than AP_2 and AP_2 is closer to N_2 than AP_1).

Here, we first compute the average wireless hops for a hybrid network. Let $d_{P-\{AP\}}$ denote the distance from a point P (P_x, P_y) to the nearest Access Point. For instance, for the scenario shown in Figure 3,

$$d_{N_1-\{AP\}} = \min\begin{cases}\sqrt{(N_{1x} - AP_{1x})^2 + (N_{1y} - AP_{1y})^2} \\ \sqrt{(N_{1x} - AP_{2x})^2 + (N_{1y} - AP_{2y})^2}\end{cases}$$

Now, the wireless path length in a hybrid network can be computed as

$$d^h(N_1, N_2) = \min\begin{cases} d_{N_1-\{AP\}} + d_{N_2-\{AP\}} \\ d_{N_1-N_2}\end{cases}$$

The average distance can now be computed as follows:

$$E\left[d^h(N_1, N_2)\right] = \int_0^1\int_0^1\int_0^1\int_0^1 d^h(N_1, N_2)\, dN_{1x} dN_{2x} dN_{1y} dN_{2y} \qquad (4)$$

The above equation is derived assuming a unit square. For a length of L, the distance has to be scaled accordingly. Using equations (1), (2) and (4), one can compute the stealthiness of a path in a hybrid optical-wireless network.

Figure 4 presents the numerical data for the above analysis for the network scenario shown in Figure 3. We consider a square network of length 1000m with a transmission range of 100m. We note that as network density increases, the *stealthiness* increases as the length of the paths decrease. Furthermore, as the number of adversary nodes (α) increases, the performance deteriorates for both wireless and hybrid cases. Hybrid cases performs better (by around 10% for α=5). However, because of omnidirectional transmissions, even a small number of adversary nodes can do significant damage.

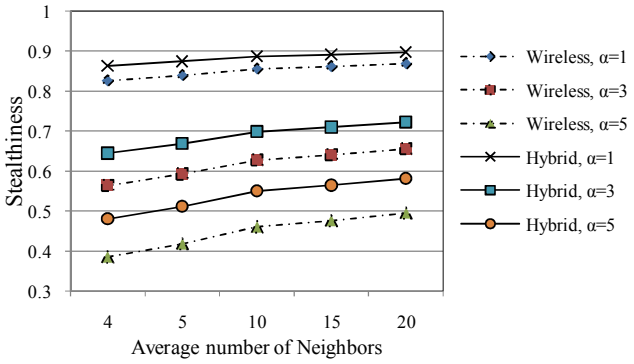


Figure 4. Performance comparision: Pure wireless Vs. Hybrid networks with omnidirectional wireless transmissions.

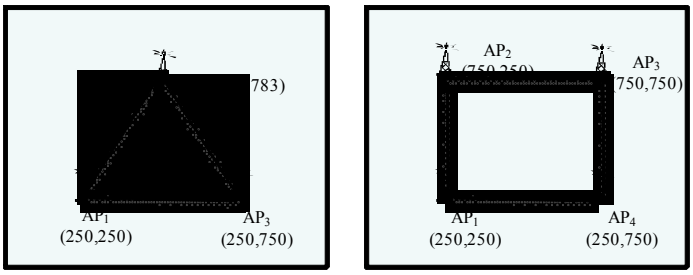
4. Stealthiness with directional transmissions

We note that using omnidirectional antennas is a poor choice for networks that desire stealthy communications. We show that tremendous improvement can be achieved

by using directional antennas. For instance, consider a directional antenna with an angle of radiation of 10^0 compared to an omnidirectional antenna whose angle of radiation is 360^0. For same transmission range, the area covered by a transmission in directional case is 36 times lesser than with omnidirectional case. Thus, there would also be a corresponding improvement in the stealthiness. The rest of the analysis to compute stealthiness is similar to omnidirectional case presented in previous sections; however, due to lack of space, we do not present them here.

PERFORMANCE STUDY

In this section, we present some analysis to study the performance of the proposed protocol. We study the most important metric – *stealthiness* - the probability of a communication message being undetected.



(a) Three APs (b) Four APs

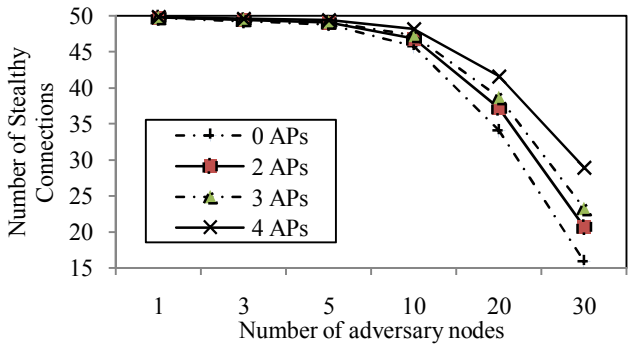
Figure 5. Network configurations studied with varying number of APs

First, we study different topologies. Apart from the topology with two APs as shown in Figure 3, we study two other topologies – with three APs and with 4 APs – as shown in Figure 5. Later, to understand the performance in random topologies, we study the relation between the *stealthiness* and the average distance from nodes to the nearest AP. We consider two network densities: 500 nodes and 200 nodes. We use directional antennas with angle θ=10^0.

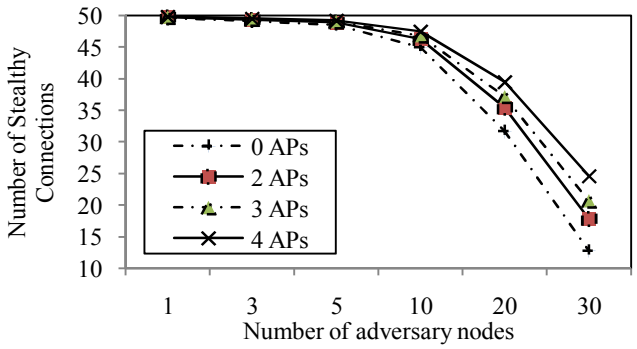
In all the scenarios, the locations of the APs are fixed as shown in the configurations. Then, the adversary red zones are randomly placed in the network area. Then, the nodes are also randomly placed. Each simulation is repeated 20 times and the average across all the runs is presented. For all the simulations, 50 source-destination pairs are randomly chosen and connections are established, exploiting the optical links where possible. A connection is stealthy if none of adversary nodes is able to overhear the wireless transmissions in a path for the connection.

Figure 6 shows the performance in known network topologies of Figure 5. We observed that, the stealthiness can be improved significantly by using optical links. For instance, with four APs and 30 adversaries, about 29 connections were stealthy on an average compared to around 15 without any optical links. Even with just one optical link, up to 6 connections could be secured.

Next, we generated some random optical configurations. For each such configuration, we ran multiple simulations. In each run, the nodes and adversaries are randomly placed. The average distance between nodes and APs is computed across all the runs and so are the results (see Figure 7). The most important observation is that increasing the number of APs does not always improve stealthiness, especially after one stage. We attribute this to the reason that, no matter how many APs are present, the two end links are always wireless in any path. We believe that by using power-controlled steered antennas to control the transmission range, this limitation could be overcome to some extent and this would be an interesting aspect to be studied further.

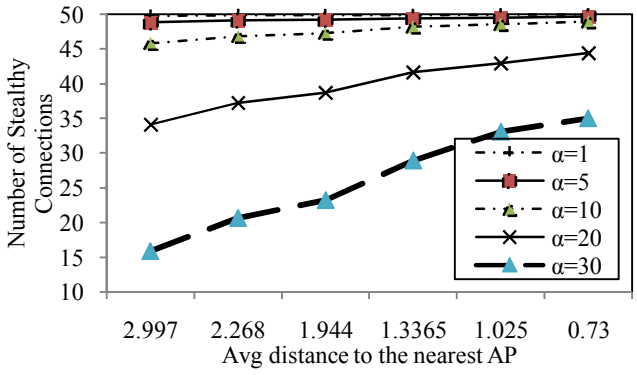


(a) 500 nodes

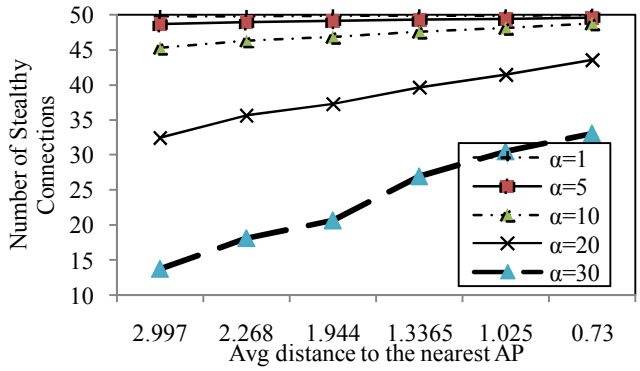


(b) 200 nodes

Figure 6. Stealthiness in various topologies for directional wireless transmissions scenario.



(a) 500 nodes



(b) 200 nodes

Figure 7. Stealthiness in unknown topologies as a function of average distance between nodes and nearest APs; directional transmission scenario

CONCLUSIONS

There is a tremendous need for networks that could perform covert operations, especially in hostile conditions. In these scenarios, the critical requirement is to be able to stealthily communicate through wireless channels. In this paper, we presented a Stealthy Routing Protocol that utilizes a hybrid network consisting of both optical and wireless communication links. As we demonstrated, SRP is able to significantly improve the *stealthiness* of communications by using optical links. SRP is able to optimize wireless communications for the best tradeoffs among, communication and security. SRP also avoids wireless propagation that overlaps with red zones, controlled by the adversary.

REFERENCES

[1] G. Zussman and A. Segall, "Energy efficient routing in ad hoc disaster recovery networks," in Proceedings of IEEE INFOCOM, 2003.

[2] K. F. Rauscher, "Wireless Emergency Response Team – Final Report for the Sep. 11 2001 NYC WTC Terrorist Attack", Oct. 2001.

[3] Y.B. Ko and N.H. Vaidya, "Medium Access Control Protocols Using Directional Antennas in Ad Hoc Networks," Proc. of IEEE INFOCOM, March 2000.

[4] N.S. Fahmy, T.D. Todd, V. Kezys, "Ad Hoc Networks with Smart Antennas Using IEEE 802.11-Based Protocols," Proc. IEEE ICC, 2002.

[5] R.R. Choudhury, X. Yang, R. Ramanathan, N. Vaidya, "Using Directional Antennas for Medium Access Control in Ad Hoc Networks,"Proc. ACM MOBICOM, Atlanta, Georgia, September 2002.

[6] Ramanathan, Redi, Santivanez, Wiggins and Polit, "Ad Hoc Networking with Directional Antennas: A Complete System Solution," IEEE Journal on Selected Areas in Communications: Special Issue on Wireless Ad Hoc Networks, March 2005.

[7] Peng-Jun Wan, "Multichannel Optical Networks (Network Theory and Applications)", Springer Publications, September 2006.

[8] Aljada, M., Alameh, K., and Al-Begain, K.Distributed Wireless Optical Communications for Humanitarian Assistance in Disasters. In Proceedings of the Third IEEE international Workshop on Electronic Design, Test and Applications, January 17 - 19, 2006.

[9] Mahdy, A. M., Deogun, J. S., and Mehta, S. K. "Broadband Optical Wireless Internet: Delay Optimization. In Proceedings of the First international Conference on Broadband Networks (Broadnets'04), October 25 - 29, 2004.

[10] Bhandari, S. and Park, E. K. "Hybrid Optical Wireless Networks". In Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, (ICN/ICONS/MCL), April 23 - 29, 2006

[11] Eric Weisstein, "Hypercube Line Picking." MathWorld - Wolfram Web Resource. http://mathworld.wolfram.com/HypercubeLinePicking.html

[12] S. De, A. Caruso, T. Chaira, and S. Chessa, "Bounds on hop distance in greedy routing approach in wireless ad hoc networks," in International Journal of Wireless and Mobile Computing, April 2005.