| | |
|---|---|
| Title | A multipath ad hoc routing approach to combat wireless link insecurity |
| Author(s) | Lee, CKL; Lin, XH; Kwok, YK |
| Citation | Ieee International Conference On Communications, 2003, v. 1, p. 448-452 |
| Issued Date | 2003 |
| URL | http://hdl.handle.net/10722/46385 |
| Rights | Creative Commons: Attribution 3.0 Hong Kong License |

# A Multipath Ad Hoc Routing Approach to Combat Wireless Link Insecurity

Clive Ka-Lun Lee, Xiao-Hui Lin, and Yu-Kwong Kwok
Department of Electrical and Electronic Engineering, The University of Hong Kong

*Abstract* -- **As wireless LAN (WLAN) technologies proliferate, it is becoming common that ad hoc networks, in which mobile devices communicate via temporary links, are built using WLAN products. In the IEEE 802.11b standard, the Wired Equivalent Privacy (WEP) scheme is used as the only measure to enhance data confidentiality against eavesdropping. However, owing to the well known pitfalls in Initialization Vector (IV) attachment in the ciphertext, the underlying 40-bit RC4 encryption mechanism in WEP is unsafe regardless of the key size. On the other hand, solutions involving replacement of RC4 by another cipher are not attractive because that may lead to reconstruction of the whole system and result in high costs as well as redevelopment of the products. In order to enhance the security on the existing development efforts, we propose a novel multipath routing approach to combat the link insecurity problem at a higher protocol layer. This approach does not require the application to use sophisticated encryption technologies that may be too heavy burdens for mobile devices. Based on our suggested confidentiality measurement model, we find that our proposed multipath ad hoc routing technique, called Secure Multipath Source Routing (SMSR), is highly effective.**

*Keywords:* **wireless ad hoc network, WEP, confidentiality, eavesdropping, multipath model, SMSR.**

## I. INTRODUCTION

Wireless networking technologies, such as WLAN (e.g., IEEE 802.11b) schemes, are rapidly proliferating, and as such, people are aggressively making use of such technologies to built *ad hoc* networks. In an ad hoc network, mobile devices wander autonomously and communicate via temporary links. Such freedom is widely envisioned to be an attractive model for many interesting applications, such as wireless gaming, location based services, etc. Specifically, each mobile device dynamically discovers other devices nearby within each other's radio range so that it can directly communicate with them. For those devices that are far apart, it relies on other devices as routers to relay packets. In this paper, we focus on ad hoc networks built based on the IEEE 802.11b short range wireless standard.

Security is a major concern in wireless networks. In the multiple access control (MAC) layer, the IEEE 802.11b standard specifies the Wired Equivalent Privacy (WEP) to enhance data confidentiality against causal eavesdropping in the sense that it provides functionality equivalent to that provided by the physical security attributes inherent to a wired medium [5]. As is standardized internationally, WEP has been widely implemented and integrated into IEEE 802.11b products for public use. Basically, WEP relies on an encryption key and a 24-bit initialization vector (IV). The encryption key is shared within all authorized users but the IV is locally handled by each source device and newly selected for every packet. Specifically, WEP uses RC4 encryption mechanism on the key and the IV to generate a 40-bit keystream. The keystream is then XORed with the plaintext for encryption to produce the ciphertext. The clear IV is finally attached and transmitted with the ciphertext. It is assumed that even though an eavesdropper can capture the ciphertext successfully, he/she cannot interpret it to the plaintext if he/she does not have the encryption key.

Indeed, eavesdropping can be a serious problem in wireless ad hoc networks. By definition, eavesdropping means any unauthorized interception of information-bearing traffic and involves various kinds of both passive and active attacks. In case of wireless ad hoc networks, since all mobile devices use the shared wireless medium, users are exposed to a potentially insecure environment and under eavesdropping in a more complex manner than wired networks. Furthermore, because ad hoc networks involve rapid changes in topology and delegated controls among all mobile devices, it is difficult to track down the eavesdropper (as illustrated in Fig. 1). Although WEP is originally designed to prevent eavesdropping, previous research has shown that, WEP has failed to meet its design goal owing to the deficiency in clear IV attachment in the ciphertext [1], [2], [4], [12]. The IEEE 802.11b design community has also admitted the failure of the WEP. The community attributes to the use of the underlying 40-bit RC4 encryption mechanism and suggests that WEP could achieve its aim to enhance confidentiality by increasing the keystream size to 104-bit or 128-bit. However, WEP is unsafe regardless of the size of the keystream due to its weakness in the initialization vector (IV).

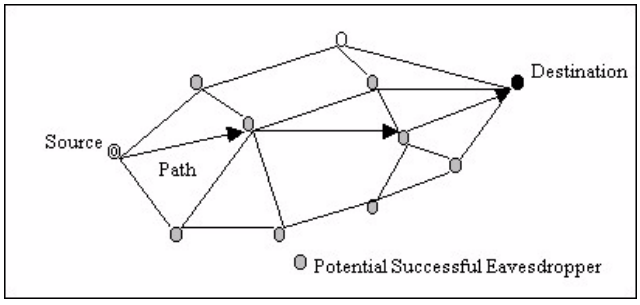


Figure 1: Eavesdropping in an ad hoc network.

The severity of the IV problem depends on the re-occurrence of the IV. For 24-bit IVs, the IVs as well as the keystreams are limited to a small space of $2^{24}$ variations. Statistical data shows that the full IV key space will be exhausted after 5 hours when 1, 500 bytes packets are transferred at 11 Mbps [12]. The keystreams will also be used up and thereafter the IV collections will be re-used. Another noticeable point is that, as is in 802.11b, the replacement of IV is optional, which could make the IV problem more threatening because of oversimplification of designs. Take a common Lucent wireless card as an example, the same predictable IV setting is repeated every initialization. A network using many wireless cards of this type will suffer a huge amount of IV collisions and also very high risk of statistical attacks [1], [2].

Another approach, which is replacing the RC4 mechanism by another cipher may lead to reconstruction of the whole system, and thus incur high investment as well as redevelopment of the wireless products. The performance of the new cipher also requires test and exploration.

In order to conserve the existing development efforts but enhance data confidentiality, we propose a novel multipath routing approach to combat the eavesdropping at the network layer. Instead of focusing on the encryption aspect, our proposed approach is to construct a multipath model to deliver data over disjoint multiple routes. Data are systematically split among the routes to minimize or even disable potential captures by unauthorized users. There are four major merits in our

0-7803-7802-4/03/$17.00 © 2003 IEEE

method:

- Our model is implemented on the network layer and thus, WEP on the MAC layer is free to be conserved or replaced. This provides high compatibility to the existing network and allows freedom for further development.
- In the proposed model, security is enhanced not only to prevent problems in IV, but also to extensively avoid various kinds of active and passive attacks.
- Splitting data among the multiple paths simplifies the security problem and provides the foundation for the upper layers for security-sensitive applications.
- Recent researches on multipath routing have been very successful and the various ad hoc routing protocols suggested are efficient in terms of delay, bandwidth, data loss, and path recovery. These advances definitely have great synergies with the proposed model in this paper.

The paper is organized as follows. We briefly outline some existing approaches in tackling the IV problem in Section II. Section III describes the framework of the multipath model. Section IV shows the design and construction of the SMSR protocol. Section V presents and discusses the simulation results. Finally, Section VI concludes this paper.

## II. Existing Solutions

It is well known that there have been two solutions proposed to solve the IV problem: increase the key size or replace the RC4 cipher. The first approach proposes to increase the size of the keystream from 40-bit to 104-bit or 128-bit. Although this method can undoubtedly avoid bruce-force attacks and prevent an eavesdropper breaking the keystream, it provides little help for WEP because with clear IV attachment, an eavesdropper can still recognize those ciphertexts using the same keystream without breaking it. Thus, a large key size is much less essential. The second approach proposes to replace the RC4 stream cipher by another cipher and therefore remove the known XOR weakness of stream cipher. An eavesdropper then cannot get the plaintext by XOR'ing two ciphertexts with the same keystream. This approach is effective to solve the IV problem, but would at the same time demands the necessity of redesigning the overall system, which may inevitably brings the consideration of the redevelopment difficulty and the high cost.

Both approaches have focused on the MAC layer in providing a solution to enhance confidentiality in ad hoc networks. However, the proposed solutions are either hard to implement or ineffective in practice. Besides, enhancing confidentiality by only encryption is not absolutely secure. With advance in computer technology, it is possible to break any encryption upon collection of sufficient information. These observations motivate our new notion to consider confidentiality enhancement in view of the network layer.

## III. The Proposed Multipath Framework

Our proposed algorithm is stimulated by the two detrimental facts with link insecurity in the single path model (thereafter is called as unipath model for simplicity), which uses only one path for data delivery:

- Huge amount of ciphertexts following the same path/link will facilitate the interception by an eavesdropper and eventually provides sufficient information for decrypting the ciphertexts, e.g. by XOR'ing two ciphertexts in WEP problem previously mentioned.
- If an encryption is broken by an eavesdropper, then a large flow of information delivered in the same path/link will be completely decrypted and exposed.

In order to minimize these two potential hazards of unauthorized decryption with the unipath model, we propose a solution implemented on the network layer to enhance confidentiality. Our approach is to construct multiple paths between a source and a destination and distribute data among the routes to minimize or even disable potential captures by unauthorized users. The idea is illustrated in Figure 2, which shows the multipath model greatly reduces the number of potential successful eavesdropper.

To achieve this aim, we studied a similar research of W. Lou and Y. Fang's theoretical multipath framework but on stable networks [8], which is the only piece of related research to our best knowledge. There are two major points with [8]:

- a secret sharing coding ensures that one can decrypt the whole message only if he/she captures a certain amount out of the total shares;
- a multipath routing algorithm can further extend the collection of cached paths by exchanging with neighbors.

In general, [8] emphasizes the encryption coding to achieve the goal in enhancing security but the model in this paper focuses more in the multipath routing algorithm. This is because in wireless ad hoc environment, even an eavesdropper is not served as a router to relay the packet, he/she can still capture packets from other mobile devices within his radio ranges. Therefore, multipath routing algorithm which affects the distribution of paths determines the effectiveness of the model in enhancing confidentiality as well. We have then built up a new model with two components in framework: a sequencing scheme and a multipath routing algorithm especially for ad hoc wireless networks.

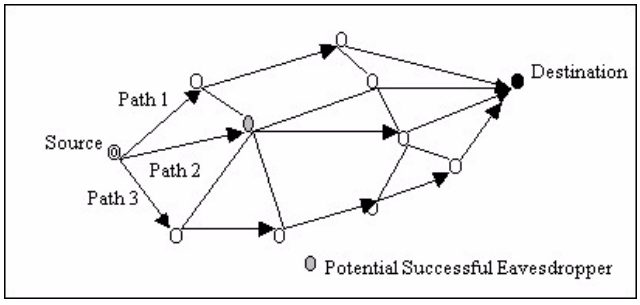


Figure 2: Eavesdropping in a multipath ad hoc network.

### A. Sequencing Scheme

Sequencing scheme concerns about how to distribute the data to different routes so as to enhance confidentiality. In other words, with sequencing scheme, even the eavesdropper can capture part of the shares, he/she cannot interpret the whole message. The model with [8], however, cannot be directly implemented in ad hoc environment where routes are limited because the secret sharing coding which tolerates the disclosure of part of shares, introduces unfavorably high redundancy to a resource limited network environment. Instead, the polynomial scheme in [8] or any other coding techniques (e.g. diversity coding [11]) can be modified to minimize unnecessary redundancies for ad hoc networks. In this paper, the approach is to rearrange the order of the data and redistribute the data among shares. An eavesdropper who captures parts of data can only interpret meaningless information. For the recipient, he/she can reconstruct the original data in the correct sequence only when all data shares are received. Since there exist many applicable encryption techniques, this paper only focuses on building a secure multipath routing algorithm.

### B. Multipath Routing Algorithm

In wireless ad hoc networks, the distribution of paths determines the confidentiality level. The further apart the routes, the harder the eavesdropper can capture the data shared. In order to achieve the best performance in confidentiality enhancement, the goal of the multipath routing algorithm in this paper is to find and utilize totally disjoint paths. The proposed mulitpath routing algorithm in [8] is based on stable networks and focuses on theoretically the number of paths found which may require further analysis for implementing in the complex ad hoc environment. On the other hand, the existing effective multipath routing algorithms usually aim at finding multiple dependent paths as backup for unipath. Very few are designed for simultaneous data transfer among multiple paths. Totally disjoint multipath routing is seldom described. Therefore, this paper contributes in constructing a secure totally disjoint multipath routing model based on one of the ad hoc routing protocol, which is discussed in more details in the coming section.

## IV. The Proposed Multipath Algorithm

Ad hoc routing protocols are classified into two main streams: table-driven and on-demand. Table-driven protocols try to maintain all route entries in a table from time to time, though some of the routes are not required. It usually requires periodic updates by control messages to prevent stale entries. In contrast, on-demand protocols initiate a route discovery only when needed, which can minimize the number of control messages but sacrifices the knowledge of the whole topology. Since the on-demand protocols are more adaptive to the changes and more efficient, we use one of the on-demand protocol, Dynamic Source Routing (DSR) [3], [6] as the base in our model.

DSR uses source routing, which means that the source knows the complete route to the destination. The route information is stored in a cache and carried in the header of every packet. If a source wants to communicate with a destination that it does not have an entry, it initiates a route discovery process by flooding a route request (RREQ) to each neighbor. After receiving the RREQ, each node checks whether it is the destination or it has the route entry in the cache. If either case fulfills, it then issues a route reply (RREP) following the reverse path to the source. If not, it continues to broadcast until a route is found or the destination is reached. In case of route breakage, the node discovering the breakage sends a route error (RRER) to the source. The source then eliminates the corresponding entry in the cache and initiates a new route discovery if necessary.

To facilitate the multipath routing mechanism, two models are studied, which are Split Multipath Routing, (SMR) [7] and Multipath Extension to DSR [9]. The SMR model was based on DSR and focused on achieving QoS routing by maintaining maximally disjoint routes. However, SMR could not be applied to serve our aim because of two major reasons. First, the model employs special forwarding techniques for finding more maximally disjoint paths in route discovery, which in our case will unfavorably introduce high number of unnecessary control messages. Second, since the major concern of the model is QoS routing, it limits the number of paths to two for each pair of connection and in case of route breakage, allows one route to continue to deliver data. These designs adversely lower the level of security. Therefore, we have to reconstruct the model for both the route discovery and route maintenance. The other model in [9] is also focused on QoS routing in DSR but on alternative paths. Although this model provides multipath discovery, it uses only one path for transmission. The alternative dependent paths in cache are used only as backup in case of route breakage. Based on our confidentiality requirement, we propose a new multipath model, Secure Multipath Source Routing (SMSR) with the details as follows:

### A. Parameters

There are two main parameters in the SMSR model which allow the system to adapt to the dynamic ad hoc environment. With suitable adjustment, the multipath model can balance between throughput and the number of disjoint paths returned to the source which determines the level of security. The two parameters are:

- Maximum waiting time, $\tau$:
  It determines the initial value of the time counter for the period that the destination should wait after receiving the first RREQ. As the value of the counter diminishes to zero, the destination should have received RREQs carrying information of different routes. The destination then selects the shortest one and the next totally disjoint ones for data delivery by sending RREP to the source in reverse routes. This parameter controls the waiting time of destination before selection and thus determines the number of routes received as well as the security level. A larger value allows a larger pool of route candidates for selection but introduces unnecessary delay. It is noticeable that this parameter is set as a reference value according to the first RREQ received. This can provide flexibility to adapt to an adverse environment or a large network.
- Maximum hop difference between the shortest path and the totally disjoint paths, $\Delta h$:
  It is another parameter required in the destination. It serves as a standard to select the routes with acceptable performance in terms of delay. After the maximum waiting time counter diminishes to zero, the destination needs to select firstly the shortest route and then all other totally disjoint paths. Although our primary aim of the multipath model is to use totally disjoint paths for security reason, the performance is also essential. This parameter regulates the hop difference versus security. Similar to $\tau$, $\Delta h$ is also set as a range relative to the shortest route serving the same purpose.

### B. Route Discovery of SMSR

Similar to DSR, SMSR uses source routing with all routing records stored in a cache and the route information carried in the packet header. If an intermediate node receives a RREQ for the first time, it broadcasts the RREQ again; otherwise, it discards the RREQ. Unlike DSR, the intermediate nodes are not allowed to send RREP to the source even it has route entries in its cache. The same procedures continue until the RREQs reach the destination. After receiving the first RREQ, instead of replying immediately with the shortest route, the destination waits for $\tau$ to receive other RREQs. Together with all RREQs coming from different routes, the destination node has the whole picture of the network and finds the suitable routes: the shortest path and then all totally disjoint paths within the value of the hop difference parameter, $\Delta h$.

With the two parameters previously mentioned, our model allows dynamic selection of routes to maintain a standard of the throughput. To implicitly control the total number of replies to prevent reply flood, the destination only sends route reply (RREP) of selected paths to the source. The source then sends data through the selected totally disjoint paths to the destination. Compared with DSR where the destination sends RREP to the source for all RREQ received, SMSR only replies the selected paths.

### C. Route Maintenance of SMSR

When one of the paths breaks, the source is notified by RRER. However, instead of initiating a new route discovery immediately, the broken path is discarded without recovering by an alternative and the remaining paths continue to deliver data. Although records of the alternative paths can be found in the cache of destination as back up, we do not use them to prevent stale entries. The remaining paths then continue to deliver data until there is only one route remains. Then, a new route discovery is initiated. Since our primary goal is to maintain at least two paths for enhancing confidentiality, another route discovery is initiated even though the last remaining path is robust.

### D. Confidentiality Measurement

To measure the confidentiality enhancement by the multipath model, a random node is selected as an eavesdropper. It performs the same as other nodes to relay packets but it collects unauthorized data within its radio range. Owing to the sequencing scheme, only that all shares of a message are captured by this eavesdropper are defined as a successful attack. There is a counter set for an eavesdropper to calculate these amount of the data successfully captured. The data later is divided by the total amount of data received successfully by the destination and thus interpreted as the interception ratio to indicate the effectiveness of the multipath model in enhancing confidentiality:

$$R_i = \frac{P_e}{P_r} \quad (1)$$

where $R_i$ is the interception ratio, $P_e$ is the total number of packets successfully eavesdropped, and $P_r$ is the total number of packets arrived at the destination.

## V. Performance Results

The performance of the following two models are evaluated and compared:

- DSR: Dynamic Source Routing which uses single path; and
- SMSR: Secure Multipath Source Routing which uses multiple paths.

Our simulation focuses on comparing the multipath model with the unipath model. The simulation scenario contains 50 mobile devices, which are randomly located in a $1200 \times 1200$ square meters area. Each node has a 300 meters propagation radius and randomly chooses a speed between 0 and 10 m/s towards a random direction. The size of the payload is 512 bytes. The maximum waiting time $\tau$ is 10 ms. The maximum hop difference between the disjoint paths and the shortest path, $\Delta h$ is 6. A random node is selected as an eavesdropper and the number of packets it captured is measured as intercepted packets for calculating the interception ratio. Cases with different payloads are simulated and the following factors are recorded for analysis:

- Interception ratio: the main indicator for the effectiveness of security enhancement by the multipath model.
- Throughput: defined as the total number of bytes received successfully by the destination per second.
- Control overhead: defined as the total number of bytes of the routing packets per second, including RREQ and RREP.
- End-to-end delay: defined as the total end-to-end delay including queuing delay and propagation delay.

Below, we show the simulation result according to the metrics mentioned.

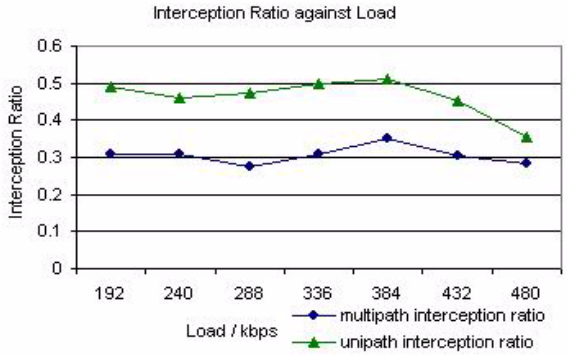


Figure 3: The system average interception ratio.

Figure 3 shows the average interception ratio of each protocol. We can observe that the interception ratio of SMSR remains about 0.3 and that of DSR stays about 0.5. The overall performance of SMSR outperforms the DSR by about 20%. Since DSR uses only one path to deliver data, an eavesdropper along the path is able to capture all information. For SMSR, the data are split and transmitted in distributed fashion, so an eavesdropper can only capture the data transmitted within his radio range and capturing all parts of the data should be extremely difficult. Since we employ the sequencing scheme, the eavesdropper can only interpret meaningless contents. This result confirms our multipath model has achieved its aim to enhance confidentiality from unipath model.

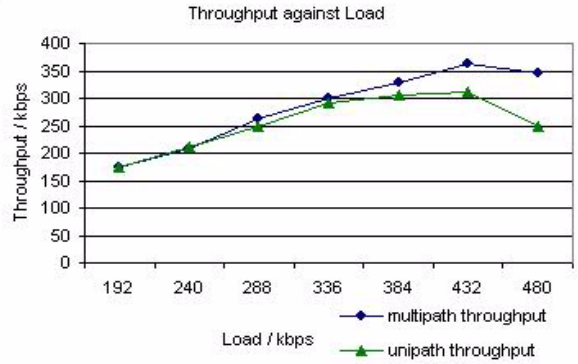


Figure 4: The system average throughput.

Figure 4 depicts the throughputs of DSR and SMSR. It is shown that the SMSR scheme outperforms DSR, especially when the load increases. In DSR, the only route used is the shortest one. When the route breaks, it tries to use a cached route overheard at first. If this attempt fails, then it will discover a new route. For the former case, intermediate nodes with cached routes send RREPs to the source to provide the cached routes. However, as DSR provides no updating methods to these caches, it is possible that the source cannot find the cached routes are stale upon route breakage until when it tries to use the involved route. This introduces more data loss as well as delay. In SMSR, multiple routes are used, means SMSR delivers more packets than DSR. Besides, in case of route breakage, even though SMSR have almost all routes break but leaving at least two available routes to the destination, the remaining routes can still continue to transmit the data. Therefore, SMSR can tolerate frequent topology changes. Although we can even achieve a higher tolerance for allowing one route

to continue to deliver data, we set the minimum available paths to be two so as to achieve our aim to share data among multiple paths for security.

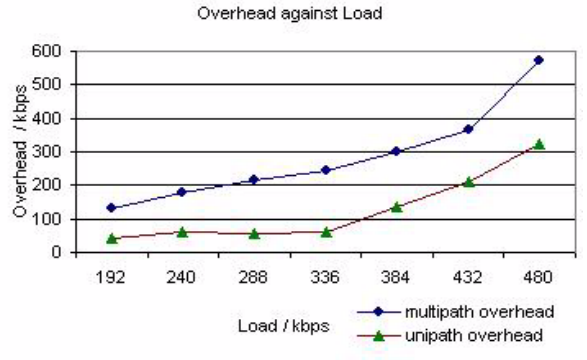


Figure 5: The system average overhead.

Figure 5 shows the routing load required for each model, which measures the protocol efficiency. It can be seen that the overheads required for SMSR is higher than that for DSR and both curves follow the similar trend as the payload increases. The result is the same as predicted brought by the overheads required for route discovery of multiple paths and packet sequencing. First, DSR allows intermediate nodes to send RREP with route information from cache directly to the source, which minimizes overhead flooding. Second, the overheads increase for sequencing controls in order to share data among multiple routes and reconstruct the data at the destination. It is also noticeable that the overhead is higher than the throughput when high load for both DSR and SMSR, which is similar to the results obtained in [7] and [10]. The major factor contributing to the increase in overheads is that as traffic increases, both DSR and SMSR experience more route disconnections and route discoveries. The source then floods the network with excessive RREQs for path reconstruction and lowers the protocol efficiency.

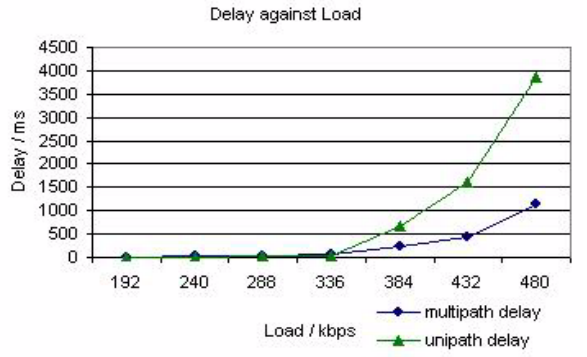


Figure 6: The system average delay.

Figure 6 illustrates the average end-to-end delay. We can observe that the overall performance of SMSR is more steady than that of DSR. Although SMSR and DSR performs equally well on light traffic, the difference becomes evident as traffic load increases. In general, DSR has shorter end-to-end delay since it always delivers data on the shortest route. However, DSR suffers longer delays in path maintenance to reconstruct routes. On the other hand, though SMSR uses longer path to deliver data, the connection remains as long as there are at least two routes left. Since the SMSR uses only totally disjoint routes, this ensures the independence of each path in case of path breakage. Breaking of one path does not necessarily affect other paths. Thus, unnecessary path recovery is minimized. This result further demonstrates the robustness of the SMSR by providing multiple routes.

In this section, the simulation results indicate that the performance of a multipath model, SMSR outweighs that of a unipath model, DSR in preventing eavesdropping. We also show the other performance benefits the multipath model bears.

## VI. Conclusions

In this paper, a multipath model is proposed to enhance data confidentiality in IEEE 802.11b based ad hoc networks, in the presence of the WEP problem. Our model SMSR is generic and can be easily applied in existing IEEE 802.11b networks. Our simulations, using the DSR protocol for comparisons, show that the successful interception ratio by eavesdropper has been lowered by over 20% with the multipath model than that with the traditional unipath model. Significant improvements in end-to-end delay and throughput are also achieved with the multipath model, especially during heavy traffic. Thus, our proposed multipath model is an effective and practicable scheme to enable secure data communications in an ad hoc network. We are currently working on the analytical and quantitative comparisons of the security impacts of different ad hoc multipath routing protocols.

## References


[1] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *Proc. MobiCom'2001*, July 2001.

[2] N. Borisov, I. Goldberg, and D. Wagner, "Security of the WEP Algorithm," *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html,* Feb. 2001.

[3] J. Broch, D. Johnson and D. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," *http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-07.txt,* IETF Internet Draft, Feb. 2002.

[4] S. Fluhrer, I. Mantin, and A. Shamir, "Weakness in the Key Scheduling Algorithm of RC4," *http://www.crypto.com/papers/others/rc4_ksaproc.ps*, 2001.

[5] The IEEE Computer Society, "IEEE Standard 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.

[6] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," in *Mobile Computing*, T. Imielinski and H. Korth (editors), Kluwer Academic, Chapter 5, 1996.

[7] S. J. Lee, and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," *Proc. ICC'01*, vol. 10, pp. 3201–3205, 2001.

[8] W. Lou and Y. Fang, "A Multipath Routing Approach for Secure Data Delivery," *Proc. MILCOM'01,* vol. 2, pp. 1467–1473, 2001.

[9] A. Nasipuri and S. R. Das, "On-demand Multipath Routing for Mobile Ad Hoc Networks," *Proc. ICCN'99*, pp. 64–70, 1999.

[10] C. E. Perkins, E. M. Royer, S. R. Das and M. K. Marina, "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks," *IEEE Personal Communications,* vol. 8, pp. 16-28, Feb. 2001.

[11] A. Tsirigos and Z. J. Haas, "Multipath Routing in the Presence of Frequent Topological Changes," *IEEE Communication Magazine,* Nov. 2001

[12] J. R. Walker, "Unsafe at Any Key Size; Analysis of the WEP Encapsulation," *http://www.cs.umd.edu/~waa/wireless.html*, Oct. 2000.