Time-based Confidentiality Enhancement Scheme for Mobile Wireless Networks

Qunwei Zheng, Xiaoyan Hong, Jun Liu, Lei Tang

Department of Computer Science,

University of Alabama, Tuscaloosa, AL 35487

Abstract

A multi-hop wireless network with highly dynamic members and mobility is vulnerable to many attacks due to the open wireless media and the difficulty of establishing strict security mechanisms. In order to send messages confidentially, one approach is to send multiple shares of the original message simultaneously through different paths. This approach has limitations when spacial multi-paths can not be found in sparse networks or geographically constrained networks. To address this problem, we propose a novel approach that exploits mobility. In our scheme, the source sends shares at different times. Due to node mobility, these shares will be routed through different intermediate nodes. It is highly unlikely that a particular intermediate node (an eavesdropper) is able to be on many of these routes and to collect enough shares to reconstruct the original message. The scheme is particularly suitable for applications that can tolerate long message delays, as studied in Delay Tolerant Networks. The paper focuses on analyzing the feasibility of this scheme. We describe a general approach to calculate the probability of nodes other than source and destination intercepting enough shares, and use the isotropic random walk model to illustrate the calculation. The scheme is further evaluated using simulation. The results show that for random walk type of mobility, the probability is small. In all, this time-based message delivery scheme provides a valuable alternative for delay tolerant applications to enhance message confidentiality.

I. Introduction

Multi-hop wireless networks for mobile nodes, e.g., mobile ad hoc networks, Mesh networks, vehicular ad hoc networks, and moveable wireless sensor networks are peer-to-peer networks where users act not only as hosts but also as routers to forward packets for others. Node mobility, frequent node join and leave, and possible long distances between nodes constitute a self-organizing and highly dynamic network. In this work, we pay attention to the challenging mobile ad hoc networks (MANETs). Such a network is vulnerable to many attacks. Possible attackers may want to eavesdrop other nodes' communication, to disrupt communication, or to deplete network resources. In some scenarios, ad hoc networks will be deployed in hostile environments, where a legitimate node could be captured and turned into malicious. Moreover, the open nature of wireless media allows these attacks to be launched with great ease. For examples, any node within the reception range of a transmission can overhear, intercept and alter transmitted messages; or, a malicious node can position itself to be within a network field and emit bogus messages. All these situations require a secure network to protect communications. One important secure aspect is the confidentiality of the messages. In this work, we study the confidentiality issue targeting at defending against the eavesdropping attacks that are interested in learning the contents of the messages.

Message confidentiality (or secrecy) can be achieved using an approach of encryption or an approach of spreading with shares. Encrypting messages before sending is a common practice. Yet for encryption to work, there must first exist keys for encryption and decryption. Both symmetric key cryptography and public key cryptography face challenges due to the dynamic nature of network members. Several early works have proposed to address the problem [3], [4], [5], [8], [15], [22], [24]. Still, there is no one-fit-all strict security mechanism. In addition, cryptographic approaches usually require additional computation time and bandwidth (for exchanging handshake needed secure credentials), which could be crucial for nodes that are resource constrained. Nodes could be compromised and a compromised node gives away all keys stored in its memory, making communication not secure. Also, cryptography cannot defend against adversaries that simply drop messages. After all, with these considerations, sending messages in MANET with needed secrecy remains a challenging issue.

Spreading a message through multiple paths is another approach to achieve secrecy. The basic idea is to split a message into multiple shares and send them to different paths. Usually, the threshold secret share scheme can be used to generate the shares. Several related secure data transmission schemes have been proposed following the idea, e.g., using node-disjoint paths [14], [16]. Multi-path routing in MANET is used to select these paths [2], [12], [19], [20]. These schemes fit well for scenarios where the space is large enough for these paths to spread apart. But they are not appropriate when a network is sparse or deployed in a restricted geographic area, where not enough node-disjoint multiple paths can be found.

Our scheme works differently. It explores node mobility by sending shares at different times. Thus it is not limited by geographical features. Notice that nodes in mobile ad hoc networks move all the time. If the time interval is large enough, two shares will be routed through different intermediate nodes. Thus it is very difficult for a node (including the eavesdropping attacker) other than the source and the destination to hear enough shares - unless it physically follows the source and the destination or it has enough collaborators in the network to help collect shares for it. A node collecting enough shares is able to reconstruct the original message by combining these shares. Not-enough shares will reveal no information about the original message.

Such a scheme has a natural fit for applications and scenarios where delay can be tolerated, similar to applications studied in Delay Tolerant Networks (DTN) [10]. It is also suitable for scenarios where multi-path does not exist or hard to find, as in a sparse network, or in a restricted geographical area. For these scenarios, our scheme can provide message secrecy, yet does not rely on the presence of in-network key distribution and cryptography approaches.

For this scheme to work, the key issue is the guarantee (with probability) that nodes other than the source and the destination will not intercept enough shares. In this paper, we introduce the scheme and analyze the feasibility of this scheme. We describe a general approach to calculate the probability, and use the isotropic random walk model to illustrate the calculation. The scheme is further evaluated using simulation. The results show that for random walk type of mobility, the probability is small. These pieces of work validate the soundness of our scheme and suggest that this time-based message delivery scheme provides a valuable alternative for delay tolerated applications to enhance message confidentiality. The paper is organized as follows. Section II introduces the security and network models, and related work. Our scheme is explained in Section III with probability analysis in Section IV. A case study with numerical results is given in Section V. We show our simulation in Section VI. Finally conclusion comes in Section VII.

II. System model and related work

A. System model

The network runs routing protocols to self-organize and to maintain conductivity for multi-hop wireless transmissions. We assume that at the time of communication, a route will be available [1]. Our scheme does not specifically require cryptographic operations in the network during message transmissions. We only assume that the two communicating parties are aware of the use of the scheme. When a mobile network has adopted a security mechanism, our scheme can co-exist with it and strengthen the security in message delivery for the applications that tolerate delay (such as applications that suitable for delay tolerant networks). For example, if the network uses message authentication code (MAC) to ensure integrity, we can secure the shares with MAC. In addition, our scheme still provides secrecy of the message content.

We assume a reasonable weak threat model, where no global monitor can be deployed. It is possible that there are more than one attackers in the network and they can collude to integrate information. But they are sparsely mingled with legitimate nodes. The attackers can eavesdrop wireless transmissions, collect data and perform traffic analysis to obtain information. In our case, they could try to correlate data packets of the same source-destination pairs and perform traffic analysis (for privacy purpose, pseudonyms can be used, but here we don't assume the protection). They can be totally quiet or appear to be normal network members, e.g, acting correctly according to the routing protocol. However, they lack the ability to follow

[1] On the other hand, threshold secret share scheme provides some reliability that allows packet losses to a certain number.

an active transmitting node continuously due to one (or more) of the following reasons: not able to locate the emitting locations, no knowledge on any specific target identities (or pseudonyms) so they will not stay close to the active nodes for a long time due to mobility or prediction of a target node's motion pattern. We assume no available visual information.

B. Related work and our contribution

Both symmetric key cryptography and public key cryptography face challenges due to the dynamic nature of network members. Several early work have proposed to address the problem. First, establishing symmetric keys between two arbitrary nodes need an infrastructure of Key Distribution Center (KDC). However, in a mobile ad hoc network, the security of KDC cannot be guaranteed. Also, when all nodes are moving, the accessibility of the KDC (to all the nodes at any time) is difficult to guarantee as well. In addition, KDC is a single point of failure. For these reasons, some symmetric key distribution schemes require physical contacts [3][22]. Still, there are scenarios where physical contacts are not practical. Another possible solution is to use key pre-distribution as studied in sensor networks [6][7]. But in an ad hoc network where nodes may join and leave at random - without a possible connection to a trusted authority - these schemes encounter difficulty. Second, in public key cryptograph, though public keys can be distributed by the node itself through some public means, it usually requires the existence of distributed and online Certificate Authorities (CAs) to verify the public keys. Based on public key cryptograph, various schemes have been proposed [4], [15], [24]. These schemes assume that a set of nodes are initialized by a trusted party before deployment. A self-organized public key management scheme was proposed in [5][8]. In this scheme, nodes issue certificates to each other based on their personal acquaintances. Each node maintains a local certificate repository. Verification of public keys is made possible by finding a certificate chain between two communicating nodes. The scheme is fully self-organized. However it provides only probabilistic guarantees.

A few works have also used multi-path routing to achieve secrecy. A secure data transmission scheme based on Rabin's Information Dispersal Algorithm (IDA) [18] was proposed in [16]. In this scheme, dispersed message pieces are routed simultaneously through a set of node-disjoint paths. The destination node reconstructs the message after receiving sufficient pieces. The authors discussed how the source can adjust the path set based on feedback from the destination so that the protocol can remain effective in an ever changing network. A similar scheme that is based on Shamir's secret sharing technique [21] was proposed in [14]. Message is divided into multiple shares and sent simultaneously through multiple independent paths. The authors discussed how to split message so that maximum security can be obtained and how to design an effective multi-path routing algorithm.

Our scheme is different from the above schemes in that those schemes utilize spatial redundancy. They can be used in scenarios where multi-paths exist. On the other hand, our scheme utilizes time redundancy. It can be used in scenarios where delay can be tolerated, or where multi-paths do not exist or are hard to find, as in a restricted geographical area. In addition, the scheme of [14] requires link encryption between neighboring nodes, the cost of which is high. Our scheme does not take such an assumption.

III. Transmit confidential data by exploiting node mobility

We use threshold secret sharing scheme to divide our messages into multiple shares. A (k, n) threshold secret sharing scheme [21] divides a secret into n shares ($k < n$). The secret can be reconstructed from k or more shares, but with less than k shares, absolutely no information about the secret is disclosed. In this section, we first give a brief overview of the secret sharing scheme and then we describe our scheme. The security analysis of the scheme will be given in the next section.

A. Secret sharing scheme

To safeguard a cryptographic key from loss, one way is to make multiple copies. By doing so the reliability increases, but the risk of leaking the key increases too. The larger the number of copies, the higher the reliability but also the risk. Secret sharing scheme on the other hand manages to enhance reliability without increasing risk. Among the various secret sharing schemes, Shamir's (k, n) threshold secret sharing [21] is the most widely cited algorithm. It starts with a secret S and divides it into n pieces in such a way that knowledge of any k or more pieces allows reconstruction of this secret, but knowledge of $k-1$ or less leaves the secret completely undetermined.

To divide the secret into n shares, we choose $k-1$ random coefficients $a_1, a_2, ..., a_{k-1}$, and a specific a_0 that equals to S, and define a $k-1$ degree polynomial $f(x) = \sum_{j=0}^{k-1} a_j x^j$. We then evaluate $f(i)$ for each $i = 1, 2, ..., n$. Each pair $(i, f(i))$ is a secret share and we have n of them. To reconstruct the secret, with the knowledge of any k pairs, we are able to use Lagrange interpolation [13] to find all the coefficients of the polynomial and the secret $S = a_0$.

Lagrange interpolation works as follows. Given k points $(x_i, y_i), i = 1, 2, ...k$ of a polynomial of degree $k-1$, the polynomial can be reconstructed as:

$$f(x) = \sum_{i=1}^{k} y_i \prod_{1 \le j \le k, j \ne i} \frac{x - x_j}{x_i - x_j}$$

Since $f(0) = a_0 = S$, the secret can be expressed as:

$$S = \sum_{i=1}^{k} c_i y_i$$

where $c_i = \prod_{1 \le j \le k, j \ne i} \frac{x_j}{x_j - x_i}$.

Some nice properties of this scheme include: it is secure; the size of each share does not exceed the size of the secret; new shares can be calculated and distributed to new users without affecting existing shares; providing a single user with more shares gives him more control over the secret.

B. Transmit data over time

At the time that the source wants to communicate with the destination securely, the source will split the message into multiple shares using the aforementioned threshold secret sharing scheme. It buffers them and sends them at different times. Fig. 1 depicts the idea. At certain locations of the source's travel path (s_1, s_2, s_3, s_4), it sends its shares. Correspondingly the destination receives the shares at locations (d_1, d_2, d_3, d_4). The success of the scheme relies on the fact that intermediate nodes are different. Suppose the source sends a share to the destination at position s_i first. The next time that it sends a share to the

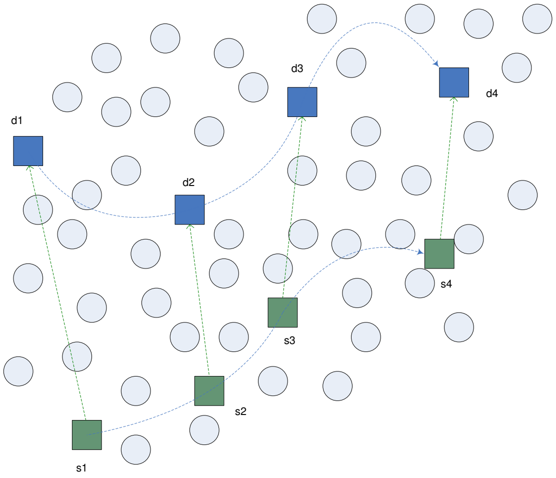

Fig. 1. Time-based data transmission scheme. Source send four shares at four different places s_1, s_2, s_3 and s_4. Destination receives these shares at d_1, d_2, d_3 and d_4 respectively. Due to mobility, shares are relayed through different nodes.

destination is at position s_{i+1}. Due to mobility, the nodes that relay the current share are different (with high probability) from the nodes that relay the next share. According to our adversary model, attacking nodes are rather weak in terms of forming a highly informative global monitoring network though collusion and information exchange by a secret channel. Thus, it is safe to say that the only nodes that can hear the shares are those that happen to be on the routing paths where the shares are relayed, or close to nodes on the paths. The destination can recover the message by the (k, n) threshold secret sharing scheme. For any other node to obtain enough shares, it must *happen* to be on enough (i.e, k) relaying paths. Since an attacking node can not deliberately follow a target node, its chance of hearing enough shares is very limited. When applications allow message delay, the time dispersion that the scheme explores brings advantages that are evident through the following analysis.

IV. Probability Analysis

In this section, we analyze the probability of an arbitrary node other than the source and the destination recovering the original message. We use the isotropic random walk model as the mobility model. Isotropic means that a node's individual steps are isotropically distributed [9]. Without loss of generality, we assume that a node needs to collect all shares (which is M) in order to recover the original message.

A. *Isotropic random walk model*

A node's random walk [9] consists of many steps. A *step* is a movement from one point to another along a straight line. The node re-selects the direction for its next step. The length of each step varies (say, following some distribution), but the time for taking each step is the same - we assume it is 1 time unit. We also assume that there is no pause between two consecutive steps.

The isotropic random walk is a random walk in which the lengths of the individual steps are isotropically distributed. The probability density function of the displacement of each step is

$$g(\mathbf{r}) = \frac{1}{2\pi|\mathbf{r}|}\omega(|\mathbf{r}|)$$

where **r** is a two dimensional vector representing displacement and $\omega(\psi)$ is the probability density function of the length Ψ of each step. There are very few cases that the probability density function for the position of a node after n steps can be evaluated explicitly. In our analysis, we will use one of those cases. In this case, the probability density function for the length Ψ of each step is [9]

$$\omega(\psi) = \frac{2\psi}{a^2}e^{-\psi^2/a^2} \tag{1}$$

where a is the sole parameter that determines the shape of the distribution. So we have

$$g(\mathbf{r}) = \frac{1}{\pi a^2}e^{-|\mathbf{r}|^2/a^2}$$

This result will be used in the following analysis.

B. *Probability analysis*

Suppose that the source sends one share to the destination every n steps. In total, it sends M shares. Notice that since both the source and the destination are moving, they send/receive shares at different locations and most likely through different paths. For a particular path, the vulnerable area that an attacking node can eavesdrop the message consists of many overlapping transmission range based circles along the irregular path. Since a shortest path tends to be geographically close to the straight line linking the source and the destination, we simplify the calculation of the vulnerable area. We approximate the vulnerable area to be a rectangle that surrounds this straight line. The rectangle has a width of $2R$ (R is a node's transmission range) and a length of the distance between the source and the destination. By this approximation, any node outside of the rectangle will not hear the share. To be able to recover the original message, a node must *happen* to be in all M rectangles at the times when the source sends the shares. There are two notes on the size of the rectangle. First, the width $2R$ is more accurate for a dense network because the path can be close to the geographical straight line linking the source and destination; for a sparse network, the width could be larger since the path may diverge away from the line. Second, the rectangle could be extended by including two half-circles of radius R to include the case that the attacker being at the outer sides of the source or the destination but within the transmission range. These considerations will make the calculation more accurate. However they do not change the essence of the analysis and the approximation. So in our analysis, we keep the size of the rectangle as $2R \times$ (the distance between the source and the destination).

We start the analysis using a simple case of $M = 3$ (see an illustration in Fig. 2). According to the isotropic random walk model, the source sends each of the three shares every n steps, at locations S_1, S_2 and S_3. The destination receives them at the corresponding locations of D_1, D_2 and D_3. The rectangles are A, B and C. Suppose that an arbitrary node N starts from a location $H(\alpha, \beta)$. It is possible that the node moves into these three areas. For this node's possible locations within the three areas, we denote A_i as an infinitesimal area centered on (x, y) within the area A; B_j and C_k are for areas B and C with similar meanings.

Let $f_{(x_0,y_0),n}(x, y)$ be the probability density function of the position of a node after n steps have been made, starting from (x_0, y_0). Then,

$$Pr\{\text{node } N \text{ is in } A_i \text{ after } n \text{ steps}\} = f_{H,n}(x, y)\, dx\, dy$$

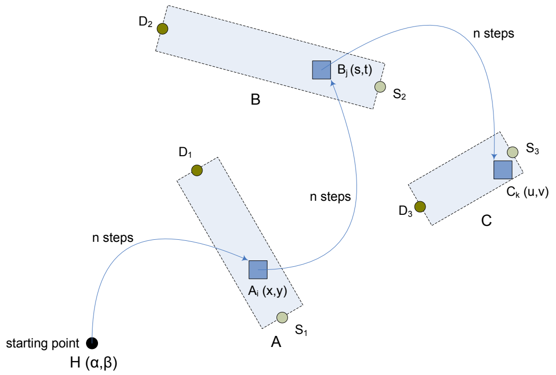

Fig. 2. Illustration of probability analysis. There are 3 rectangle areas which are decided by the positions of the source and the destination (at different time). An arbitrary node starts from H. What is the probability that with every n steps it enters area A,B and C consecutively.

$$Pr\{\text{node } N \text{ is in } A \text{ after } n \text{ steps}\} = \int_A f_{H,n}(x,y)\,dx\,dy$$

$$Pr\{\text{node } N \text{ is in } A_i \text{ after } n \text{ steps AND is in } B_j \text{ after another } n \text{ steps}\}$$

$$= \quad f_{(x,y),n}(s,t)\,ds\,dt \cdot f_{H,n}(x,y)\,dx\,dy$$

So,

$$Pr\{\text{node } N \text{ is in } A \text{ after } n \text{ steps AND is in } B \text{ after another } n \text{ steps AND is in } C \text{ after another } n \text{ steps}\}$$

$$= \int_C \int_B \int_A f_{(s,t),n}(u,v)\,du\,dv \cdot f_{(x,y),n}(s,t)\,ds\,dt \cdot f_{H,n}(x,y)\,dx\,dy$$

Similar result can be acquired if there are M shares (and thus M rectangle areas), by just doing M iterated integrals.

According to the isotropic random walk model we introduced in the previous section, we have

$$f_{(0,0),n}(x,y) = \frac{1}{\pi n a^2} e^{-(x^2+y^2)/na^2} \tag{2}$$

This result can be extended to the case when the node starts from an arbitrary point (x_0, y_0)

$$f_{(x_0,y_0),n}(x,y) = \frac{1}{\pi n a^2} e^{-((x-x_0)^2+(y-y_0)^2)/na^2} \tag{3}$$

So we have

$$\begin{aligned} & Pr\{\text{node } N \text{ is in } A \text{ after } n \text{ steps} \\ & \quad \text{AND is in } B \text{ after another } n \text{ steps} \\ & \quad \text{AND is in } C \text{ after another } n \text{ steps}\} \\ = & \int_C \int_B \int_A \frac{1}{\pi n a^2} e^{-((u-s)^2+(v-t)^2)/na^2}\, du\, dv \\ & \quad \cdot \frac{1}{\pi n a^2} e^{-((s-x)^2+(t-y)^2)/na^2}\, ds\, dt \\ & \quad \cdot \frac{1}{\pi n a^2} e^{-((x-\alpha)^2+(y-\beta)^2)/na^2}\, dx\, dy \end{aligned} \tag{4}$$

In fact, the above analysis represents a general approach. It can be justified as follows. First, the areas of A, B and C can be any shapes or any rectangles (with their width being $2R$). For a possible area shape we should be able to calculate the probability with suitable integrals. Second, the locations of A, B and C are decided by the moving trajectories of the source and the destination. As long as A, B and C are given, we can calculate the probability. Here we have the random walk mobility model, and A, B and C could appear anywhere (with certain probability) in the field. In addition, when the source sends M shares (and thus M rectangle areas), a similar result can be acquired by doing M iterated integrals. Finally, it is easy to see that in a general case where there are X adversarial nodes, the probability of at least one adversarial node hearing all the shares is

$$1 - \Pi_{i=1}^{X}(1 - p_i)$$

where p_i is the probability of the ith adversarial node entering all those areas at the right time.

V. A Case Study with Numerical Results

In this section, we provide numerical analysis for a case where the source and the destination move along two parallel lines with equal velocity. The rest of the nodes move following isotropic mobility model. Such a choice does not lose generality since it is still an example of an isotropic random network. We use this case to illustrate how we apply the above analytical approach. More general situations of the source and destination movements will be simulated in the next section. The network is given in Fig. 3. Here, the distance between the source and the destination is l. So all the rectangles are of width $2R$ and length l, which are shown in the figure as shaded parts. The source moves along the x axis to the right. The destination moves along the line $y = l$ to the right. We assume the length η of each step of the source/destination is the same (which is different from other nodes whose step length varies according to the distribution). So in every n steps, they move $\epsilon = n\eta$.

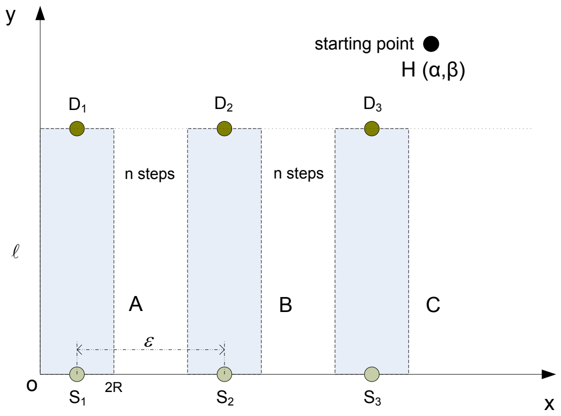

Fig. 3. Source and destination move in parallel with the same speed. Their distance is l. Rectangles A, B and C are of size $2R \times l$. Source and destination move distance ϵ every n steps.

Denote the function to be integrated in formula (4) as $h(x, y, s, t, u, v)$, that is

$$\begin{aligned} & h(x, y, s, t, u, v) \\ = \; & (\frac{1}{\pi n a^2})^3 \cdot e^{-\frac{1}{na^2}[(x-\alpha)^2+(y-\beta)^2+(s-x)^2+(t-y)^2+(u-s)^2+(v-t)^2]} \end{aligned}$$

Thus, rewriting (4), we have

$$\begin{aligned} & Pr\{\text{node } N \text{ is in } A \text{ after } n \text{ steps} \\ & \quad \text{AND is in } B \text{ after another } n \text{ steps} \\ & \quad \text{AND is in } C \text{ after another } n \text{ steps}\} \\ = \; & \int_C \int_B \int_A h(x, y, s, t, u, v)\, du\, dv\, ds\, dt\, dx\, dy \end{aligned}$$

$$= \int_0^l dv \int_{2\epsilon}^{2\epsilon+2R} du \int_0^l dt \int_{\epsilon}^{\epsilon+2R} ds \int_0^l dy \int_0^{2R} h(x,y,s,t,u,v)\, dx \tag{5}$$

In the following, we investigate how the different parameters, such as the distance between the source and the destination, influence the probability of an arbitrary node hearing all the shares. We consider an arbitrary node starting from position $H(\alpha, \beta) = H(550, 450)$. The transmission range $R = 250$ meters and the distance $l = 1000$ meters; Shares are sent every $n = 2$ steps; The step length of the source/destination is $\eta = 300$ meters. During this period, the source and the destination move $\epsilon = n\eta = 600$ meters. The expected value of the length Ψ of each step of an arbitrary node can be calculated from (1) as

$$E[\Psi] = \int_0^{+\infty} \psi\omega(\psi)\, d\psi \tag{6}$$

$$= \frac{1}{2}a\sqrt{\pi} \tag{7}$$

Let $a = 400$. This gives the expected step length of an arbitrary node $E[\Psi] \approx 354$ meters, which is comparable to source/destination's step length $\eta = 300$ meters. With these values, we calculate formula (5) by changing one parameter at a time and keep all the other parameters default.

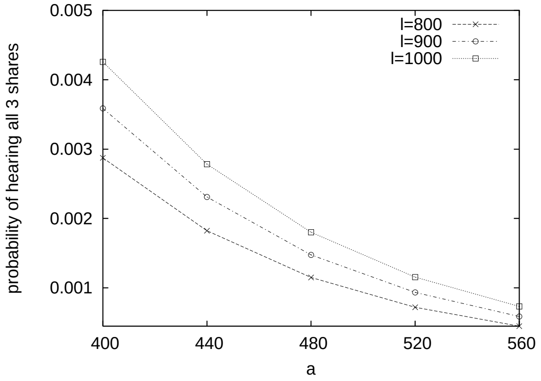

Fig. 4. Probability decreases as a increases. As l increases, probability increases too.

Fig. 4 shows that as a (the parameter in Formula (1)) increases, the probability of hearing all 3 shares decreases. Here, a controls expected step length of an arbitrary node (formula (7)). Since the time taken for each step is a constant (1 time unit), increasing a means increasing the node's speed. Please notice that in order to keep the system consistent, we also increase the source/destination's speed at the same

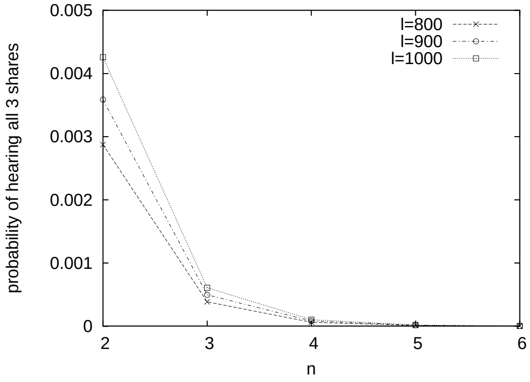

Fig. 5. Probability decreases as n increases.

rate. This means that if we double a (an arbitrary node's average speed doubles), we double η too (the source's and the destination's speed doubles). Thus Fig. 4 indicates that as nodes' speeds increase, the probability of an arbitrary node hearing all the shares decreases. This will be attested by our simulation. Fig. 4 also tells us that as the distance between the source and the destination (l) increases, the probability increases. This is because the rectangle becomes larger and it is easier for the adversarial node to enter these areas.

Fig. 5 shows that as n, the number of steps moved before a share is sent, increases, the probability of hearing all 3 shares decreases. Since the time taken for each step is constant, increasing n means that the time interval between sending two consecutive shares increases. This reduces the chances for an arbitrary node to be in the areas to collect the shares. The influence from l suggests the same trend as seen from the previous figure.

VI. Simulation

We run simulation in QualNet^{TM} to evaluate our scheme. QualNet^{TM} is a packet level simulator for wireless and wired networks, developed by Scalable Network Technologies Inc [1]. The simulated network has 300 nodes moving in an area of $5000m \times 5000m$. *Random Waypoint* model is used to simulate node mobility [11]. According to the model, a node travels to a randomly chosen location with a certain speed picked from the range of [minSpeed, maxSpeed] and stays for a while before moving to another random location. In our simulation, the speed is controlled in such a way that mobility decaying problem is minimized [23] (by setting the minSpeed larger than zero), and nodes will not pause at the locations that they choose. Initially nodes are randomly deployed in the area. At the network layer, AODV routing protocol is used to select routing paths for data communications [17]. The distributed coordination function (DCF) of IEEE 802.11 is used as the MAC layer with virtual carrier sensing for unicast packets. The transmission range is $250m$.

We run CBR (Constant Bit Rate) sessions to send shares of a message. A *session* is a lasting connection between a source/destination pair. In a CBR session, the source sends several 32-byte packets to the destination at the constant rate of one packet each time interval (e.g., 10 seconds). The packets are the shares in our scheme: one packet is one share. In the simulated mobile ad hoc network, a packet will be forwarded by several intermediate nodes before it is delivered to the destination.

We collect statistics from all these nodes except the source and the destination for a session in question. This presents the worst case for our scheme, because we treat all the nodes as attackers - when they forward a packet, they obtain the content of the packet. We investigate the chance of a particular node to hear a certain number of shares that belong to the same session. The results are averages over all the nodes and sessions. The simulation time is 900 seconds.

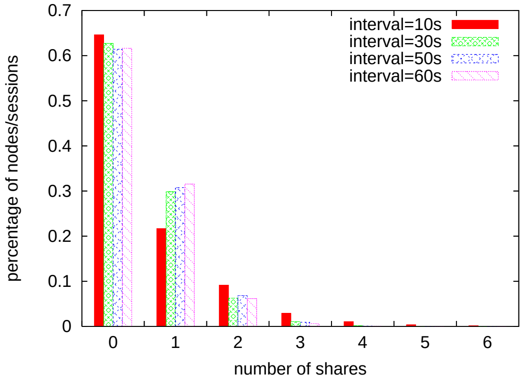

Fig. 6. Distribution with different intervals.

In the first set of simulation, we show the probability distribution of shares being heard by an arbitrary

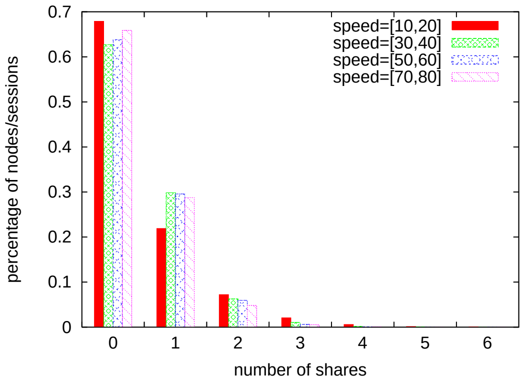

Fig. 7. Distribution with different speed ranges.

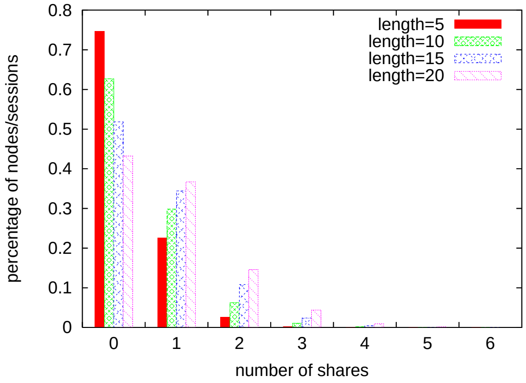

Fig. 8. Distribution with different numbers of shares.

node. Here, we set the default CBR sending interval as 30 seconds, number of shares as 10, number of sessions as 50, and the speed range $[30, 40]$ m/s. In the simulation, we will change CBR sending interval (Fig. 6), speed range (Fig. 7), and the number of shares per session (Fig. 8). These figures show distributions of the percentage of nodes hearing a specific number of shares averaging over the 50 sessions. They also show the percentage of sessions during which a node hears a specific number of shares averaging over the 300 nodes. Notice that these two are in fact the same. From these figures, it is clear that a large portion of nodes hear no share at all. Moreover, the percentage of nodes that hear more than 2 shares is very low, no matter what interval lengths or motion speeds are (Figs. 6 and 7). For Fig. 8, when the sessions send fewer shares, the probabilities of hearing no share are higher than the ones sending more shares, e.g., the case of sessions having only 5 packets. In correspondence, if a session has more shares, the probabilities of leaking one or more shares are higher as expected. However, considering that the (k, n) scheme may also set a higher k for reconstructing the original message, the probabilities do not necessarily suggest a higher success ratio for an attacker. As an opposite example, the probability of hearing 4 packets in the case of session length being 5 is not zero, though it becomes zero for leaking all the 5 packets. For other session lengths, the percentages of nodes hearing more than 6 shares are all zeros. In fact, none of the figures show data beyond 6 shares because they are all zeros.

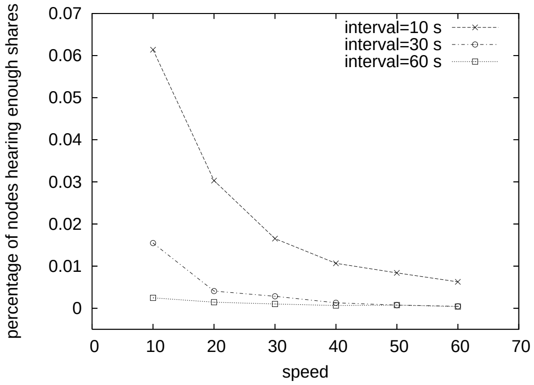

Fig. 9. percentage of nodes hearing enough (3 or more) shares drops as node speed increases and as sending interval increases.

In the second set of simulation, we investigate how the sending interval and the speed influence the ability of an arbitrary node hearing enough shares. We pick the parameters of threshold secret sharing as $(k, n) = (3, 5)$, i.e., a message is divided into 5 shares and hearing 3 or more shares will be able to recover the original message. So here "enough" shares means 3 or more shares. These values are chosen only for the purpose of illustrating the changing trend of the probability.

The results of the second set of simulation is shown in Fig. 9. There are 100 sessions in the network. The node's speed ranges increase as $[10, 20]$ m/s, $[20, 30]$ m/s, $[30, 40]$ m/s, $[40, 50]$ m/s, and $[50, 60]$ m/s. Notice that the coordinates in the x axis show only the minimum speeds of their corresponding speed ranges. The three curves in the figure are corresponding to the sending intervals of 10 seconds, 30 seconds and 60 seconds respectively. The figure shows that as node speed increases, the percentage of nodes who hear at least 3 shares drops. It also shows that as time interval increases, the percentage of hearing at least 3 shares drops too. These results are consistent with our expectation and also with the numerical solutions in the previous section.

In all, the simulation results suggest that the probability of hearing enough shares is low. In practice, in order to achieve better protection, a larger n (and k) should be used: it is evident from the first set of simulation (where $n = 10$) that when we increase n (and k), the hearing probability approaches zero.

VII. CONCLUSION

We presented and analyzed a data transmission scheme that enhances message secrecy for mobile ad hoc networks. The scheme explores node mobility through delaying the transmissions of message shares over a long period of time, resembling the application scenarios of Delay Tolerant Networks. We presented probability analysis, and used an isotropic random walk mobility model as a case study. We further used simulation to evaluate the scheme with different parameters and network scenarios. The results suggest that the probability for an attacker to hear multiple shares at different locations is small under the mobility model. The analysis and evaluation validate that the delayed transmission scheme is a valid alternative to preserve the message secrecy for delay tolerant applications and also for network scenarios where spacial multi-paths are not feasible. Work in progress includes analytical work on parameter selection and simulation comparisons with more mobility models.

REFERENCES

[1] Qualnet. *http://www.scalable-networks.com/*.

[2] Z. H. A. Tsirigos. Multipath routing in the presence of frequent topological changes. In *IEEE Communication Magazine*, Nov 2001.

[3] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *NDSS*, 2002.

[4] Y. S. C. Zhang and Y. Fang. Modeling secure connectivity of self-organized wireless ad hoc networks. In *27th IEEE International Conference on Computer Communications (INFOCOM 2008)*, AZ,USA, April, 2008.

[5] S. Capkun, J.-P. Hubaux, and L. Buttyan. Mobility helps security in ad hoc networks. In *MobiHoc '03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 46–56, New York, NY, USA, 2003. ACM Press.

[6] H. Chan, A. Perrig, and D. X. Song. Random key predistribution schemes for sensor networks. In *IEEE Symposium on Security and Privacy*, pages 197–, 2003.

[7] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *ACM Conference on Computer and Communications Security*, pages 41–47, 2002.

[8] J.-P. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pages 146–155, New York, NY, USA, 2001. ACM Press.

[9] B. D. Hughes. *Random Walks and Random Environments, VOLUME 1: Random Walks*. Oxford Science Publications, 1995.

[10] S. Jain, K. Fall, and R. Patra. Routing in a delay tolerant network. In *ACM Sigcomm*, 2004.

[11] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. In Imielinski and Korth, editors, *Mobile Computing*. Kluwer Academic Publishers, 1996.

[12] J. H. K. Wu. Performance study of a multipath routing method for wireless mobile ad hoc networks. In *the 9th international symposium on modeling, analysis and simulation of computer and telecommunication system*, 2001.

[13] D. Knuth. *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*. Addison-Wesley, Reading, Mass., 1969.

[14] W. Lou, W. Liu, and Y. Fang. Spread: enhancing data confidentiality in mobile ad hoc networks. In *INFOCOM 2004*, pages 2404–2413, Hong Kong, China, March 2004. IEEE.

[15] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang. Ursa: ubiquitous and robust access control for mobile ad hoc networks. *IEEE/ACM Trans. Netw.*, 12(6):1049–1063, 2004.

[16] P. Papadimitratos and Z. J. Haas. Secure data transmission in mobile ad hoc networks. In *WiSe '03: Proceedings of the 2003 ACM workshop on Wireless security*, pages 41–50, New York, NY, USA, 2003. ACM Press.

[17] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pages 90–100. IEEE, February 1999.

[18] M. O. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *J. ACM*, 36(2):335–348, 1989.

[19] B. Radunovic, C. Gkantsidis, P. Key, and P. Rodriguez. An optimization framework for opportunistic multipath routing in wireless mesh networks. In *27th IEEE International Conference on Computer Communications (INFOCOM 2008)*, AZ,USA, April, 2008.

[20] M. G. S-J. Lee. Split multipath routing with maximally disjoint paths in ad hoc networks. In *ICC'01*, 2001.

[21] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[22] F. Stajano and R. J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Security Protocols Workshop*, pages 172–194, 1999.

[23] J. Yoon, M. Liu, and B. Noble. Random waypoint considered harmful. In *Infocom 2003: Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, pages 1312–1321. IEEE Press, 2003.

[24] L. Zhou, F. B. Schneider, and R. V. Renesse. Coca: A secure distributed online certification authority. *ACM Trans. Comput. Syst.*, 20(4):329–368, 2002.