IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 18, 2016, accepted December 4, 2016, date of publication December 9, 2016, date of current version January 23, 2017.

Digital Object Identifier 10.1109/ACCESS.2016.2637887

Direction Density-Based Secure Routing Protocol for Healthcare Data in Incompletely Predictable Networks

JIAN SHEN[1], (Member, IEEE), CHEN WANG[2], CHIN-FENG LAI[3], (Senior Member, IEEE), ANXI WANG[2], AND HAN-CHIEH CHAO[4], (Senior Member, IEEE)

[1]Jiangsu Engineering Center of Network Monitoring and the Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China
[2]School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China
[3]Department of Engineering Science, National Cheng Kung University, Tainan 701, Taiwan
[4]Department of Electrical Engineering, National Dong Hwa University, Hualien 97401, Taiwan

Corresponding author: H.-C. Chao (hcc@mail.ndhu.edu.tw)

This work is supported in part by the National Natual Science Foundation of China under Grant 61672295, Grant 61300237, Grant U1536206, Grant U1405254, Grant 61232016, and Grant 61402234, in part by the National Basic Research Program 973 under Grant 2011CB311808, in part by the Natural Science Foundation of Jiangsu province under Grant BK2012461, in part by the research fund from Jiangsu Technology and Engineering Center of Meteorological Sensor Network in NUIST under Grant KDXG1301, in part by the research fund from Jiangsu Engineering Center of Network Monitoring in NUIST under Grant No. KJR1302, the research fund from Nanjing University of Information Science and Technology under Grant S8113003001, in part by the 2013 Nanjing Project of Science and Technology Activities for Returning from Overseas, in part by the 2015 Project of six personnel in Jiangsu Province under Grant R2015L06, in part by the CICAEET fund, and in part by the PAPD fund.

ABSTRACT Healthcare data are becoming increasingly important in the life of people. By utilizing healthcare data in a proper and secure manner, the elderly may avoid some sudden diseases, whereas young people can monitor their health condition. In the hospital, for certain sizes of detection objects, an effective method of data transmission becomes very significant. In view of the movement of patients in the hospital, we introduce a type of network called incompletely predictable networks to describe such scenarios. The patients move in a certain trend or are only active in a certain limited range. To achieve high performance when transmitting healthcare data in such networks, a novel protocol called the direction density-based secure routing protocol is proposed in this paper. Both the moving direction and the influence of node group movement are considered. The novel protocol innovatively takes the density of the node moving direction into consideration, which makes full use of the relationships among the moving individuals. Moreover, the design of the secure routing with authenticated message transmission ensures secure healthcare data communication. The simulation shows that our protocol achieves a high packet delivery ratio with low overhead and end-to-end delay.

INDEX TERMS Direction density, incompletely predictable networks, secure routing protocol, healthcare data.

I. INTRODUCTION

Personal health has aroused great concern among modern residents. The great demands of social development and the urgent need for continuous monitoring and early warnings for personal health promote the further development of techniques for processing and transmitting health data.

A large amount of healthcare data exists in wireless body area networks (WBANs) [1], [2]. WBANs are a type of wireless communication network that take the human body as the center, with components including wearable or embedded sensors, a portable personal terminal and a remote control center. Different types of sensors can be important collectors of human physiological data. These sensors send information to the remote control center through the personal terminal. The remote control center analyzes and processes the data to meet different application requirements. Due to the characteristics of being inexpensive, portable, and providing real-time monitoring, WBANs have wide application prospects in fields such as medical and healthcare, emergency rescue, smart homes, military, entertainment, tracking and positioning, and so forth [3]–[6]. At present, WBANs have important theoretical significance and application value in the fields of the prevention and treatment of various diseases and the health care of the elderly and disabled. Most importantly, the socialization and popularization of WBANs cannot be separated from the secure and reliable communication protocol. Researchers have devoted considerable efforts to realize this aspect [7], [8].

Contemporary medical treatment is more inclined to real-time monitoring of the treatment objects. Abundant and various data collected by sensor nodes attached to or implanted in the human body contain vast medical information, which might help medical staff to improve treatment methods [9], [10]. If one wants to provide unified care to the patient in a certain range, the transmission of healthcare data will become a vital problem. The quality of life of city inhabitants is a crucial element of national stability, prosperity and social harmony. Currently, the intelligence concept has been popular among the people. Intelligent health care is an important component of the intelligent trend [11], [12]. The real-time monitoring and effective early warning of various diseases can no longer be separated from the intelligent health monitoring platform. In this scenario, individuals in the network (medical staff or patients) only move within a small range. Consequently, the network constructed by objects being observed in a certain area can be treated as an incompletely predictable network or the so-called IPN. IPNs are thoroughly discussed in [13]. IPNs refer to a type of network in which individuals move in a certain range or with a particular trend. The characteristics of IPNs are relatively small amounts of topology changes and partly predictable movement tendencies.

Aiming at solving the particular problems of IPNs and the transmission of healthcare data, a novel protocol named the direction density-based secure routing protocol (DDSRP) is proposed. Based on the situation of node mobility and position, we attempt to transmit messages efficiently and safely. In the field of traditional ad hoc networks, some protocols that utilize the information of nodes' moving direction have been presented by some researchers. However, none of these works have mentioned the significance of direction density. Direction density can not only master the directions of nodes but also the movement characteristics of a certain area or the node group movement. This work is the first time in which the concept of direction density has been proposed.

Moreover, healthcare data have extremely high security requirements [14]. Thus, ensuring secure healthcare data communication is necessary. DDSRP provides secure routing with mutual authentication mechanisms to safely transmit healthcare data. This makes DDSRP able to ensure communication efficiency and privacy between different individuals in the network. We compare DDSRP with ad hoc on-demand distance vector (AODV) routing [15] and dynamic organized topology-based routing using the greedy algorithm (GrD-OTBR) [13] to show its performance in the simulation part of this paper. Moreover, security analysis of the protocol is also presented in the same section.

The remainder of this paper is organized as follows. In Section II, some up-to-date related works that utilize moving direction to design routing protocols or that use new methods to provide secure routing services are listed. In Section III, the model of a hospital healthcare data transmission and the model of IPNs are given. In Section IV, the detailed definition of direction density is presented. In Section V, the entire process of implementing the secure routing protocol is described in detail. In Section VI, the security analysis and simulation results are stated. Finally, a conclusion is drawn in Section VII.

II. RELATED WORK

In the current century, research on network routing protocols is increasing. Many excellent routing protocols have been proposed to solve the routing problems in network communication [16]–[18]. Some researchers have broken the original limit of the design of network routing protocols with new technologies. According to the characteristics of mobile ad hoc networks, some researchers have made full use of the node mobility features, among which the nodes moving direction is a more popular research area.

Kouah *et al*. [19] selected a proper relay node to be the next hop in terms of moving direction, moving speed and distance to the sink of the candidate nodes. The protocol aims at achieving a high delivery ratio, short path length and low overhead. The proposed protocol is associated and compared with GPSR.

Gupta *et al*. [20] also utilized the metrics of moving direction, successful delivery and latency records, as well as the recent proximity to the direction, to adapt to post-disaster scenarios. A 4-tier network architecture was proposed in this work to describe post-disaster scenarios.

Ghafoor *et al*. [21] attempted to establish a reliable routing link in vehicular ad hoc networks, incorporating the relative direction between the source vehicle and candidate vehicles, the distance to the destination and the beacon reception rate. By weighting the three parameters, the protocol selects the optimal intermediate vehicle.

Pandey *et al*. [22] proposed a distance and direction-based location-aided routing (DD-LAR) protocol. They developed a mathematical model to evaluate DD-LAR in terms of path duration and hop count metrics.

Li and Ko [23] investigated two types of routing costs: position-only-dependent costs such as hops, throughput or energy and traffic-proportional costs such as energy-load balancing. Two numerical approaches for determining the routing direction, the fast marching method and the finite element method, were also investigated in this work.

In addition, healthcare data communication security is also widely investigated. Many remarkable secure routing protocols and great security mechanisms have been proposed [24]–[32].

Yao *et al*. [33] proposed a trust routing based on the social similarity (TRSS) scheme, which finds routes in terms of a nodes trustworthiness. This protocol can achieve remarkable performance against many types of attacks. However, there is room for improvement in terms of detection accuracy and cost.

Yao *et al*. [34] proposed a secure routing with decode-and-forward relaying. The protocol was proven to achieve nearly the same performance as an exhaustive search.

Luo *et al*. [35] presented a symmetric lookup-based routing algorithm referred to as symmetric-chord to prevent networks from being attacked by malicious nodes. They claimed to achieve an effective approach for routing security.

Ahmed *et al*. [36] presented a trust and energy aware secure routing protocol (TESRP) for WSNs. The statement in this paper indicates that TESRP can ensure data dissemination and balance out energy consumption.

It is beyond dispute that the information of moving direction is applied to design good routing protocols in different ways and with different technical means [37], [38]. However, there is still considerable room for utilizing a node's moving direction. Additionally, communication security in the medical field is also of considerable importance. This indicates that proposing a routing protocol for healthcare data transmission and communication needs to consider routing performance and communication security simultaneously. In this paper, a novel secure routing protocol based on the direction density of movement is proposed for networks that have nodes moving in a small range or with a certain tendency.

III. MODEL DESCRIPTION

Incompletely predictable networks are networks whose topologies are relatively stable over a long period of time, resulting from nodes with a fixed activity range in the networks. Fig. 1 illustrates this case of IPN in practice. This figure shows a real-time monitoring system for user's health in IPNs. Different patients in different wards move around their wards in limited ranges. Medical staff can be aware of the physical conditions of the patients through the network and the data handled in the background. In this system, the sensor nodes receive physiological data of users, which are collected and transmitted to the remote-control center and medical staff. According to the up-to-date information, the medical staff implement real-time monitoring of users. The remote-control center is responsible for the long-term monitoring of user health status. By regularly sending health reports to healthcare workers, the remote-control center helps medical staff to make further judgments of the user health status and provide further treatment plans.

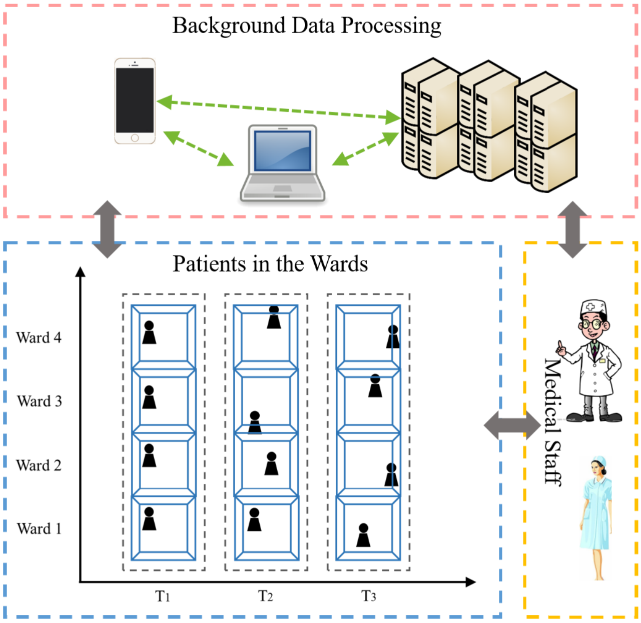


FIGURE 1. An example of IPN in wise medical.

The abstract model of IPNs is illustrated in Fig. 2. In detail, Fig. 2(a) shows the topological distribution of nodes at a specific moment, whereas the time-space graph in Fig. 2(b) shows the locations of the nodes and the relationship between them in the form of a sequence of snapshots in the network. Note that some notations used in our protocol are presented in Table 1.

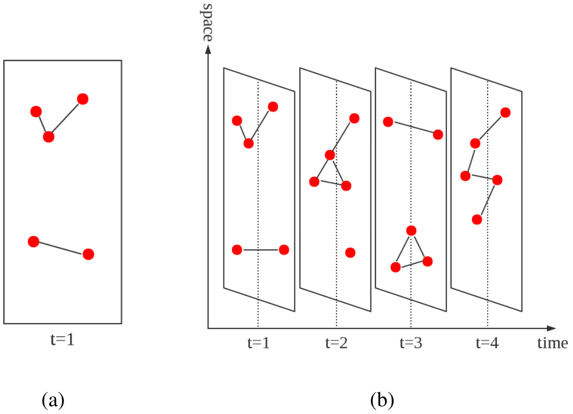


FIGURE 2. A time-evolving network: (a) a snapshot of the network and (b) time-evolving topologies of the network.

TABLE 1. Notations in our protocol.

Symbol	Description
θ	Direction angle
ρ_D	Direction density
$\mathcal{H}$	Division order
Z_S	The source zone
Z_D	The destination zone
Z_{TR}	The target relay zone
DR	Density representation node
Z_{TS}	The temporary source zone
Z_{TD}	The temporary direction zone
(T_i, t_i)	The static key pair
(E_i, e_i)	The ephemeral key pair
$\mathcal{K}$	A shared secret key
P	The generator of the group of points over a finite field

IV. DIRECTION DENSITY

A "good" moving direction is generally considered to be the direction of a node that is moving toward the position of the destination node. To better study a node's moving direction, we first define the concept of direction angle, on the basis of which the concept of direction density is defined.

A. DIRECTION ANGLE

The definition of direction angle is given in Definition 1.

Definition 1 (Direction Angle): The direction angle is defined as the angle between the direction of node movement and that of message transmission.

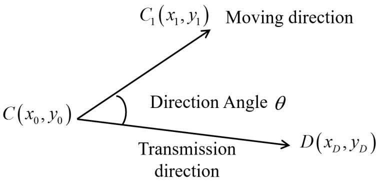


FIGURE 3. Example of direction angle.

In detail, we define the candidate node that might be selected to be the relay node as C and the destination node as D in Fig. 3. We utilize the location change of node C in a short period of time to define the moving direction. Specifically, as shown in Fig. 3, the coordinates of C are $C\,(x_0, y_0)$ a period of time ago, and then the coordinates become $C_1\,(x_1, y_1)$. The vector $\overrightarrow{CC_1}$ actually indicates the moving direction; in other words, $\overrightarrow{CC_1} = (x_1 - x_0, y_1 - y_0)$. The coordinates of destination D are $D\,(x_D, y_D)$. Similarly, the vector $\overrightarrow{CD}$ indicates the direction of message transmission; in other words, $\overrightarrow{CD} = (x_D - x_0, y_D - y_0)$. From the above definition, it is not difficult to see that the direction angle can be calculated using Eq. (1).

$$\theta = \arccos\left(\frac{\overrightarrow{CC_1}\cdot\overrightarrow{CD}}{\left|\overrightarrow{CC_1}\right|\cdot\left|\overrightarrow{CD}\right|}\right) \tag{1}$$

The definition of direction angle is an important criterion for determining the direction density in the later phase of the protocol. To a certain extent, the size of the direction angle reflects the probability that the target node can receive the information transmitted by the node as a forwarding node. When a node moves away from the destination node, we consider that it is not suitable to be utilized as a forwarding node.

B. DIRECTION DENSITY

The direction density of each zone is defined in Definition 2.

Definition 2 (Direction Density): The direction density of a zone is defined as the proportion of the nodes with smaller direction angles among all nodes in the zone.

The direction density ρ_D can be presented as in Eq. (2). Here, note that every node has its own direction density; thus, when nodes want to authenticate each other for communication, the value of direction density (ρ_D) is utilized as a part of message authentication code (MAC).

$$\rho_D = \frac{\sum \textit{nodes with small direction angle in the zone}}{\sum \textit{nodes in the zone}} \tag{2}$$

In this paper, we define a node with a direction angle that is less than or equal to 45° as the node with a proper direction angle.

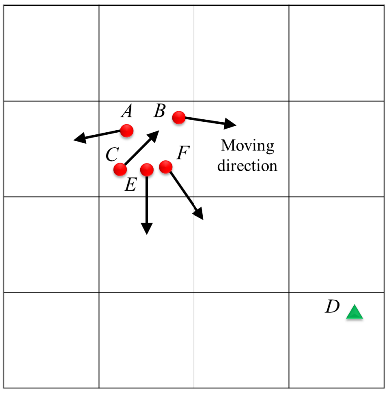


FIGURE 4. Example of direction density.

As shown in Fig. 4, nodes A (1,1,130), B (1,1,40), C (1,1,89), E (1,1,30), and F (1,1,5) are in the same zone. It can be determined through calculations that B, E, and F have relatively small direction angles (less than 45 degrees), whereas A and C are moving away from D. According to Definition 2, the direction density of this zone $\rho_D = 3/5 = 0.6$.

V. DIRECTION DENSITY-BASED SECURE ROUTING PROTOCOL

To facilitate the description, we assume that the entire network region is a rectangular area with randomly distributed nodes. Fig. 5 shows the specific process of the proposed protocol.

At the very beginning of the process, the division order of the entire network is artificially defined. By dividing the entire network area into several parts, the direction density of each part can be calculated if necessary. During each round of the protocol, a target relay zone, which is en route from the source zone (temporary source zone) to the destination zone (temporary destination zone), is selected. It has the highest value of direction density among all the candidate zones. The target relay zone will be treated as a temporary source or destination zone and be utilized in the next round of routing. When a message is transmitted from one node to another, the two nodes need to authenticate each other. Generally, DDSRP can be divided into two parts. In the routing selection part of DDSRP, there are three very significant phases, which will be stated in detail, followed by the secure routing part of the routing protocol. To introduce the process of the protocol more clearly, a specific case analysis is presented after the introduction of all parts.

A. THE ROUTING SELECTION PART OF THE PROPOSED PROTOCOL

The three phases in this part are the division and localization phase, density judgment phase and forwarding phase. Detailed descriptions of these three phases are given in the following.

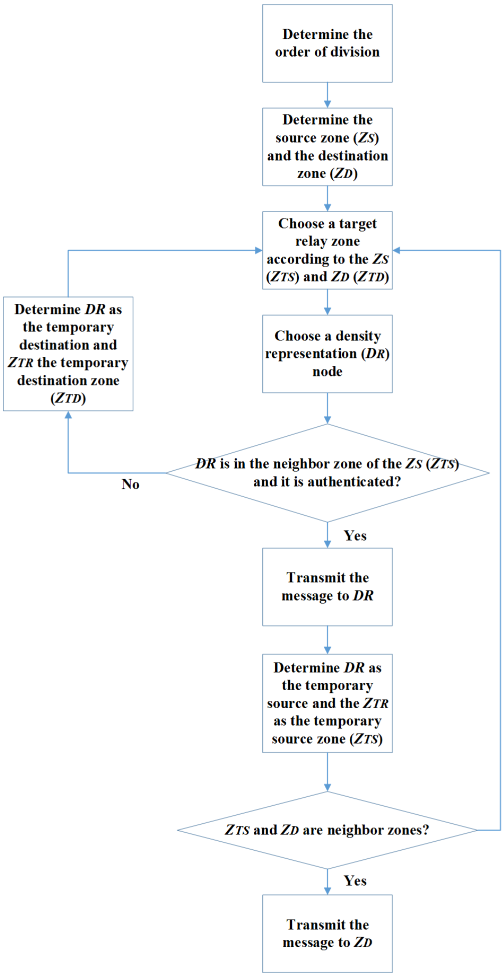

Determine the order of division
Determine the source zone (Z_S) and the destination zone (Z_D)
Choose a target relay zone according to the Z_S (Z_{TS}) and Z_D (Z_{TD})
Determine DR as the temporary destination and Z_{TR} the temporary destination zone (Z_{TD})
Choose a density representation (DR) node
DR is in the neighbor zone of the Z_S (Z_{TS}) and it is authenticated?
No
Yes
Transmit the message to DR
Determine DR as the temporary source and the Z_{TR} as the temporary source zone (Z_{TS})
No
Z_{TS} and Z_D are neighbor zones?
Yes
Transmit the message to Z_D

FIGURE 5. The flow chart of the proposed protocol.

1) DIVISION AND LOCALIZATION PHASE

The division and localization phase can be viewed as the initial stage of the entire protocol. According to the total number of nodes in the network and the size of the network area, the entire area is divided into several pieces of suitable size. We utilize the order $\mathcal{H}$ of division to indicate the number of parts that the entire area is divided into. For instance, if $\mathcal{H}$ equals 4, the entire network area is divided into 16 parts, as shown in Fig. 6.

Subsequently, each area position in the entire network will be defined in the form of coordinates. In this paper, the zone at the upper left corner of the entire network is defined as the (0,0) zone. In Fig. 6, S is located at the (1,1) zone, while D is located at the (3,3) zone. The zones that contain the source node and destination node are called the source zone (Z_S) and destination zone (Z_D), respectively. For a certain destination node, each node has a deterministic triple T_i^t $(x - axis, y - axis, DA)$ at each time t. S has such a triple T_S^t $(1, 1, \theta)$.

Determination of order $\mathcal{H}$: The value of $\mathcal{H}$ determines the node density of each zone in the network. The selection of $\mathcal{H}$ must be moderate. A $\mathcal{H}$ that is too large leads to a node density of each zone that is too low. If the number of nodes in each zone is too small, the direction density will become meaningless. In contrast, if the value of $\mathcal{H}$ is not large enough, the direction density cannot fully represent the moving attribute of the nodes in the entire zone because of too many nodes being divided into one zone. The method for calculating $\mathcal{H}$ is expressed by Eq. (3).

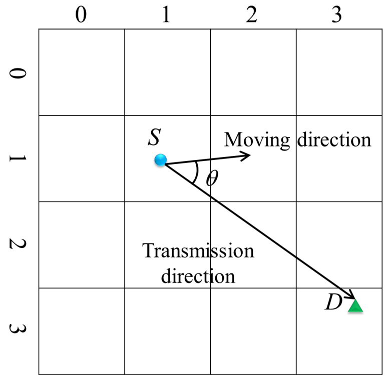


FIGURE 6. Illustration of the division and localization phase.

$$\mathcal{H} = \sqrt{\frac{\rho \cdot G}{k}} \tag{3}$$

where G represents the size of the network area and ρ represents the node density of the network. The size of each zone is denoted by k. For instance, the division order $\mathcal{H}$ equals 4, and the entire network size is 16. The node density is set as 1. The number of nodes in each zone might be $k = \frac{16}{4^2} = 1$.

2) DENSITY JUDGMENT PHASE

In this phase, we need to address the following issues. First, the standard for determining the direction density of a zone needs to be clarified. Second, the protocol should provide a clear specification for which zones need to be used for comparison with each other in terms of direction density.

First, according to Definition 2, the number of nodes with direction angles less than or equal to 45° relative to the total number of nodes in a single zone is defined as the direction density of that zone. This helps to find the zone that has the largest proportion of nodes with small direction angles.

The second issue to be addressed is to define the zones that need to be judged. In this paper, all zones with horizontal and vertical coordinates that are greater than or equal to that of Z_S and Z_D (except for both the source and destination zones) are considered. In these zones, the zone with the maximum direction density is selected, which is called the *target relay zone* or Z_{TR}.

3) FORWARDING PHASE

The setting of this phase is to allow the message to be transmitted to the target relay zone that is set during the previous phase. Through the nodes in this zone, messages are then expected to be sent to the destination zone.

Density Representation Node: The density representation (DR) node is one node that is randomly selected from the nodes in the target relay zone to represent all nodes in that zone as a relay node. For a selected target relay zone, a random target point is set as shown in Fig. 7. The node that is closest to the random target will be chosen as the DR node. In Fig. 7, it is very clear that node C_5 will be chosen as a DR node. In the secure part of DDSRP, the authentication between two adjacent DR nodes is presented.

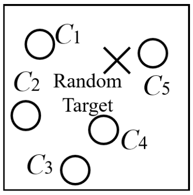


FIGURE 7. The selection of a density representation (*DR*) node.

Neighbor Zone: Before stating the working principle of this phase, there is a concept that needs to be defined. The concept of neighbor zone is given in Definition 3

Definition 3 (Neighbor Zone): Two different zones that share a boundary line or a vertex call each other the neighbor zone; in other words, they are neighbor zones.

This definition is used to determine whether the two zones are adjacent. If two zones are adjacent, then they are neighbor zones and no additional target relay zones need to be discovered for message forwarding. The owner of the message will find a suitable path through one or more hops to forward the message to the DR node or the destination zone.

Temporary Source and Destination Zone: During the transmission process, when it is discovered that the chosen Z_{TR} and Z_S are not neighbor zones, a novel Z_{TR} needs to be selected on the path from Z_S to the previous Z_{TR}. Therefore, we consider the previous Z_{TR} to be a temporary destination zone or Z_{TD}.

However, when the message is transmitted to the Z_{TR} and Z_{TR} is not the neighbor zone of Z_D, we still need to determine a new Z_{TR} on the path from the previous Z_{TR} to Z_D. In that case, the previous Z_{TR} is considered to be a temporary source zone or Z_{TS}.

4) STATEMENT OF A SPECIAL CIRCUMSTANCE

Note that not all situations in which Z_S (Z_{TS}) and Z_D (Z_{TD}) are not neighbor zones require selecting a new Z_{TR} again. There is one exception where only one zone exists between Z_S (Z_{TS}) and Z_D (Z_{TD}). In other words, if the horizontal coordinates of the two zones are the same but the vertical coordinates have a difference of 2, it is not necessary to find Z_{TR} for the communication between the zones. The zones with the same horizontal coordinates and vertical coordinates with a difference of 2 have the same characteristic.

B. THE SECURE ROUTING PART OF THE PROPOSED PROTOCOL

As we all know, healthcare data are very private and important, as such data contain personal physiological parameters and are related to personal health and even life safety [39]. In our protocol, after the target node is found following the routing selection part, authentication needs to be implemented in the routing between the nodes. If the target node is authenticated, the message transmission will continue. Otherwise, the selected node will be abandoned and a sub-optimal node will be chosen to be the target. Assume that there is a node DR_i that wants to transmit a message to DR_j. We need to ensure that the communication between the two nodes is secure. In other words, DR_i needs to know whether the node that is accepting his message is DR_j. DR_j also needs to know whether the source of the message is secure. For this reason, DR_j and DR_i need to authenticate each other prior to transmitting any healthcare data, as illustrated in Fig. 8. Reference [40] utilized a similar method to achieve secure communication between a patient's controller and healthcare worker's device. The authenticated key agreement method is proven to be secure. Note that a message authentication code algorithm denoted as MAC is needed, such as HMAC. It is utilized to provide key confirmation. $\mathcal{H}_1$ is a key derivation function. To provide a practical example, $\mathcal{H}_1$ can be SHA-1. Note that DR_i and DR_j have two public keys to achieve forward secrecy: a static one and an ephemeral one. The static public key will be bound to the individual for a period of time, generally through the use of certificates. Each run of the protocol generates a new ephemeral public key. The static key pair of DR_i is denoted as (T_i, t_i), whereas the ephemeral key pair of DR_i is denoted as (E_i, e_i). Here, $T_i = t_iP$ and $E_i = e_iP$. Similarly, DR_j takes (T_j, t_j) and (E_j, e_j) as its static key pair and ephemeral key pair, respectively. Note that the value of the direction density ρ_D is used as a part of MAC. The authentication process is illustrated in Fig.8.

1) DR_i generates $e_i \in_E [1, n - 1]$, computes the point $E_i = e_iP$ and sends it to DR_j.
2) a) DR_j generates $e_j \in_E [1, n - 1]$ and computes the point $E_j = e_jP$.
   b) DR_j computes $s_j = (e_j + \overline{E_j}t_j) \bmod n$ and $K = hs_j(E_i + \overline{E_i}T_i)^2$. If $K = \mathcal{O}$, DR_j terminates the protocol run with failure. $\mathcal{K}$ is the shared secret key.
   c) DR_j utilizes the x-coordinate value x of the point K to compute a shared key $\mathcal{K} = \mathcal{H}_1(x)$.
   d) DR_j computes $\mathrm{MAC}_{\mathcal{K}}(2, \rho_{Dj}, \rho_{Di}, E_j, E_i)$ and sends this and E_j to DR_i.
3) a) DR_i computes $s_i = (e_i + \overline{E_i}w_i) \bmod n$ and $K = hs_i(E_j + \overline{E_j}T_j)$. If $K = \mathcal{O}$, DR_i terminates the protocol run with failure.
   b) DR_i utilizes the x-coordinate value x of point K to compute a shared key $\mathcal{K} = \mathcal{H}_1(x)$.
   c) DR_i computes $\mathrm{MAC}_{\mathcal{K}}(2, \rho_{Dj}, \rho_{Di}, E_j, E_i)$ and verifies that this equals what was sent by DR_j.

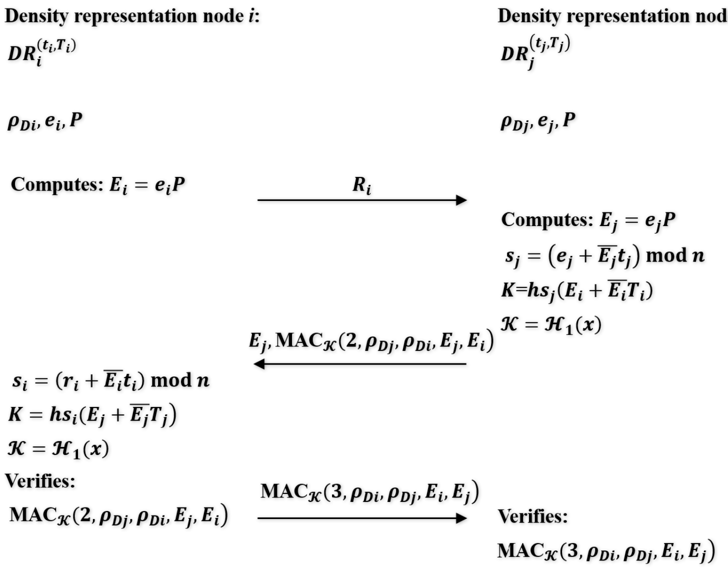

Density representation node i:
$DR_i^{(t_i,T_i)}$
ρ_{Di}, e_i, P
Computes: $E_i = e_iP$
R_i
Density representation node j:
$DR_j^{(t_j,T_j)}$
ρ_{Dj}, e_j, P
Computes: $E_j = e_jP$
$s_j = (e_j + \overline{E_j}t_j) \bmod n$
$K = hs_j(E_i + \overline{E_i}T_i)$
$\mathcal{K} = \mathcal{H}_1(x)$
$E_j, \mathrm{MAC}_{\mathcal{K}}(2, \rho_{Dj}, \rho_{Di}, E_j, E_i)$
$s_i = (r_i + \overline{E_i}t_i) \bmod n$
$K = hs_i(E_j + \overline{E_j}T_j)$
$\mathcal{K} = \mathcal{H}_1(x)$
Verifies:
$\mathrm{MAC}_{\mathcal{K}}(2, \rho_{Dj}, \rho_{Di}, E_j, E_i)$
$\mathrm{MAC}_{\mathcal{K}}(3, \rho_{Di}, \rho_{Dj}, E_i, E_j)$
Verifies:
$\mathrm{MAC}_{\mathcal{K}}(3, \rho_{Di}, \rho_{Dj}, E_i, E_j)$

FIGURE 8. Authentication message transmission between density representation nodes.

d) DR_i computes $\mathrm{MAC}_{\mathcal{K}}(3, \rho_{Di}, \rho_{Dj}, E_i, E_j)$ and sends this to DR_j.

4) DR_j computes $\mathrm{MAC}_{\mathcal{K}}(3, \rho_{Di}, \rho_{Dj}, E_i, E_j)$ and verifies that this equals what was sent by DR_i.

5) The shared secret is K, where $K = hs_i(E_j + \overline{E_j}T_j) = hs_j(E_i + \overline{E_i}T_i) = hs_is_jP$.

After the five steps, DR_i and DR_j successfully authenticate each other. Through this method, the healthcare data can be transmitted to authenticated individuals in the network.

C. AN EXAMPLE OF THE ROUTING PROCESS

To describe the process of the entire routing protocol more clearly, we assume two different situations, as shown in Fig. 9, to illustrate the specific process.

It is clearly observed from Fig. 9 that the source node is located at zone (1,1) and the destination node at (3,3). Therefore, zone (1,1) is called the source zone Z_S and (3,3) is called the destination zone Z_D. According to the routing algorithm proposed in this paper, the direction densities ρ_D of the seven zones, which are (2,1), (3,1), (1,2), (2,2), (3,2), (1,3) and (2,3), are calculated and compared. The zone with the highest value of ρ_D is chosen to be the target relay zone Z_{TR}. In the first case in Fig. 9, zone (1,2) is selected to be Z_{TR}. One of the nodes in zone (1,2) is selected as the density representation node DR_1. The Z_S and Z_{TR} where the node DR_1 is located have a common boundary, which indicates that the two zones are neighbor zones. Thus, node S directly finds the path of the message to the node DR_1. When S finds that it cannot communicate with DR_1 directly, it selects a suitable relay node to forward the message to DR_1. Once the message has been received, DR_1 takes itself as the temporary source node and D as the destination node. Z_{TR} where DR_1 is located is viewed as a temporary source zone Z_{TS}. The phases

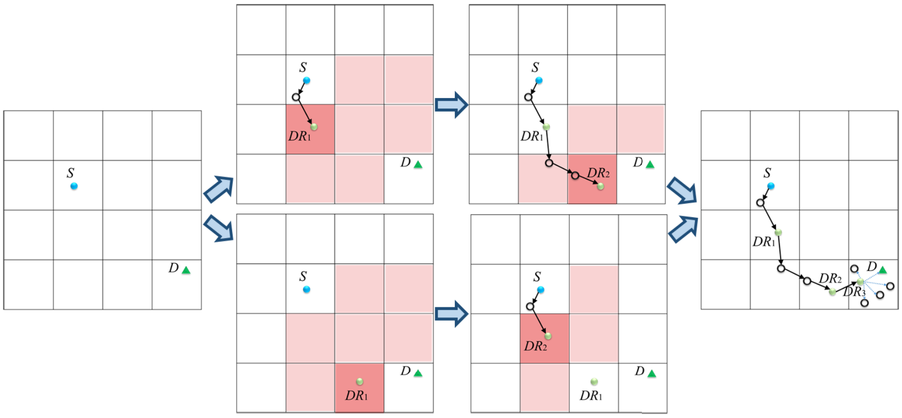


FIGURE 9. An example of the routing process.

that have been previously experienced will be repeated. Zone (2,3) is selected as Z_{TR} from zones (2,2), (3,2), (1,3) and (2,3). DR_2 is randomly chosen from the nodes in zone (2,3). The zone of node DR_1 and the zone of node DR_2 have a common vertex, and thus, they are confirmed as the neighbor zones. After a two-hop relay, the message is sent to DR_2 from DR_1. At this moment, the zone where DR_2 is located is the neighbor zone of the destination zone Z_D. The message will be sent to any node in Z_D.

In the other case, in the first round to find the Z_{TR}, from zones (2,1), (3,1), (1,2), (2,2), (3,2), (1,3) and (2,3), zone (2,3) is the one with the highest value of ρ_D. One node in this zone is randomly chosen as DR_1. According to the judgment of the zone coordinates, Z_S and the first Z_{TR} are not neighbor zones. Subsequently, the second round to find a new Z_{TR} starts immediately. The scope of the density judgment includes zones (2,1), (1,2), (2,2) and (1,3). Clearly, zone (1,2) is selected as Z_{TR}, and a node in Z_{TR} is chosen as DR_2. Under the current circumstances, Z_S and the second Z_{TR} are neighbor zones. Therefore, the message is transmitted from the source node S to DR_2. Meanwhile, the first and second target relay zones are now the neighbor zones. Thus, the route from DR_2 to DR_1 is also established. When the message is delivered to DR_1, the following message transmission that occurs is identical to the first case.

VI. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

In our simulations, one floor of a hospital covering an area of one square kilometer is taken as the simulation object. There are approximately 20, 50, 100 or 150 patients on the floor in the different simulations. The patients move in their own way in the range of the certain floor. The simulations are implemented with ns-2 [41]. Some parameters utilized in our simulations are listed in Table 2.

TABLE 2. Parameters used in simulation.

Parameter	Value
Number of nodes	20, 50, 100, 150
Mac	IEEE 802.11 DCP
Traffic source	CBR for UDP-based traffic
Node speed	0∼5m/s
Propagation model	Two-ray ground reflection
Simulation time	1000 seconds

The movement model of the patients can be described by IPNs, as briefly summarized by the following three points:

- The node number is limited in the network;
- The nodes are initially located at fixed positions called basic positions;
- The nodes move in a limited range around the basic positions if they need to.

The following metrics utilized in [42] are taken as the performance measurements to analyze our routing protocols:

Packet Delivery Ratio: The definition of packet delivery ratio is the number of delivered packets from all generated packets.

Normalized Routing Overhead: Normalized routing overhead is the number of routing packet transmissions in all data packet transmissions.

Average End-to-end Delay: The representation of average end-to-end delay is the average number of the time intervals between delivered packets and generated packets.

To summarize, the performance metrics discussed in this paper are packet delivery ratio, normalized routing overhead and average end-to-end delay. These three metrics are discussed in terms of the effect of node density.

A. SECURITY ANALYSIS OF OUR ROUTING PROTOCOL

In addition to recording data, an adversary can alter, intercept and replay messages in an active attack. An authentication mechanism is used to achieve a trusted communication environment by convincing a controller that the nodes he is communicating with are indeed the nodes they claim to be. The analysis of the concrete security properties withstanding active attacks that we are concerned about in the presented protocol is shown as follows.

1) MALICIOUS INSIDER RESISTANCE

Malicious insiders [38] are misbehaving discharged patients. In the proposed protocol, the authentication is similar to the protocol proposed in [40], which has been proven to be secure. From DR_i's perspective, the only one except himself who can compute $\text{MAC}_{\mathcal{K}}(2, ID_j, ID_i, R_j, R_i)$, the $\mathcal{K}$ in which is someone who can compute K, must be DR_j. Thus, DR_i has the assurance that DR_j has computed $\mathcal{K}$ and K. For this reason, the authentication message transmission between DR_i and DR_j provides explicit key authentication and can resist attacks from malicious patients.

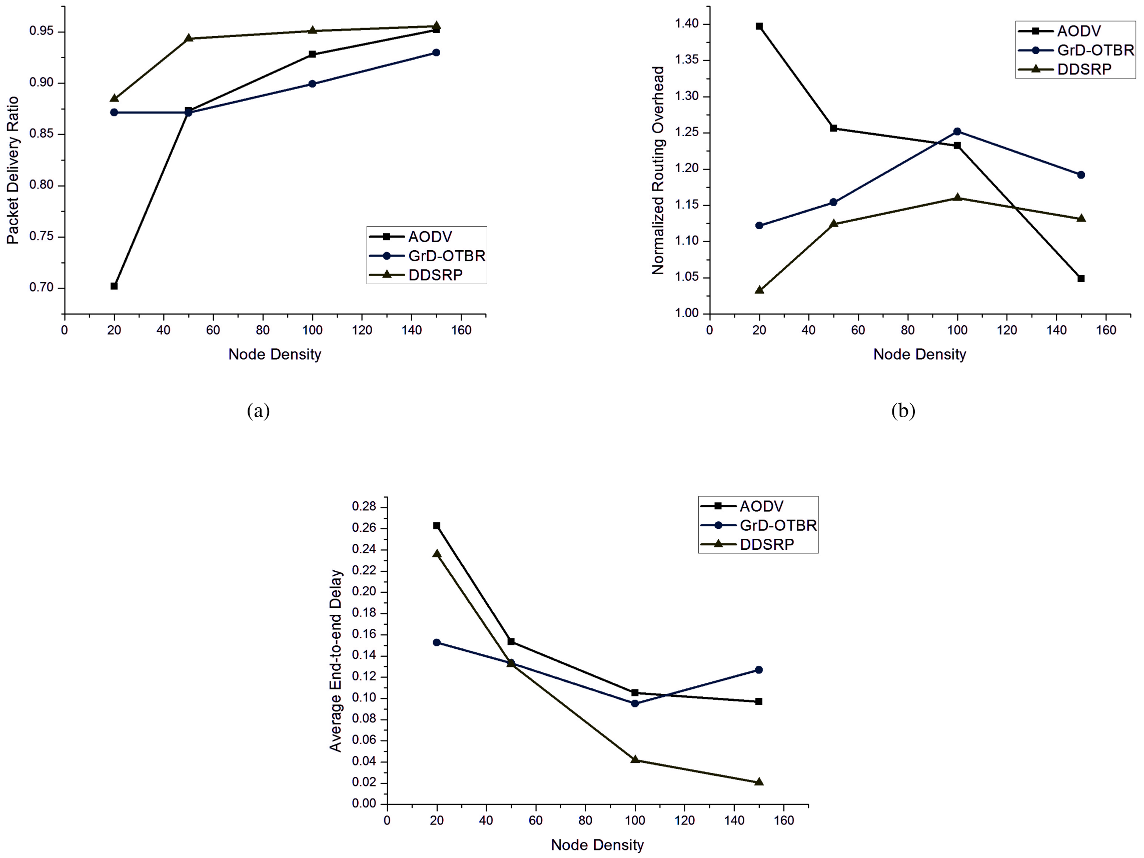
2) IMPLICIT KEY AUTHENTICATION

Implicit key authentication is a fundamental security property, which implies that only the users who A wants to agree upon a common key with are able to compute a key. In our protocol, nodes communicate with the authenticated message transmission process. Only DR_j, the object DR_i wants to communicate with, can compute the key. It is clear that our protocol provides implicit key authentication.

B. PERFORMANCE ANALYSIS OF OUR PROTOCOL

Based on the theoretical analysis, we use the ns-2 simulator to implement the simulation and comparison among AODV, GrD-OTBR [13] and our proposed protocol. The version ns-2.35 is used, and the protocols are run on Ubuntu 12.04.

We considered different node densities in a fixed-size network to determine the performance of the protocols. As mentioned above, 20 nodes, 50 nodes, 100 nodes and 150 nodes are set with fixed moving ranges and transmission ranges. The packet delivery ratio, normalized routing overhead and average end-to-end delay are taken into consideration as the



(a)

(b)

(c)

FIGURE 10. Performance vs node density: (a) packet delivery ratio, (b) normalized routing overhead, and (c) average end-to-end delay.

performance metrics. The data of each parameter of AODV, GrD-OTBR and the proposed protocol DDSRP are plotted in Fig. 10.

In general, it is not difficult to see that, compared with the other two protocols, the proposed protocol is very competitive.

Fig. 10(a) illustrates that the packet delivery ratio of AODV rapidly increases as the number of nodes increases. In contrast, the delivery ratios of GrD-OTBR and DDSRP remain at a high level despite the changing node density. It is not difficult to determine that the performance of DDSRP in terms of packet delivery ratio remains better than that of GrD-OTBR, and the reason for this is that DDSRP makes full use of the information of node moving direction. The mastery of the hot spots with high direction density is helpful for the further route discovery. However, when the node density is low, the reference value of the direction density is reduced accordingly, which is the reason for the relatively low ratio when the node density is 20.

As shown in Fig. 10(b), there is a substantial improvement of the normalized routing overhead of DDSRP compared with the other two protocols. In particular, in the case of a high node density, DDSRP improves the problem of high overhead of GrD-OTBR. This is because the DDSRP only needs to calculate and record the real-time direction density of each area. Obtaining the topology of the entire network, which is required in GrD-OTBR, is avoided in DDSRP. This allows a considerable amount of transmission and storage overhead to be saved.

According to Fig. 10(c), the variation trend of the average end-to-end delay of DDSRP is similar to that of AODV. In other words, the larger the node density is, the lower the delay will be. The reason for the low delay of DDSRP is that nodes in each area are viewed as a group, which can greatly capitalize on the regional advantages of node movement. Through the aforementioned methods, improved transmission efficiency leads to a low end-to-end delay.

To summarize, in the situation described by IPNs, the novel protocol appears to be more appropriate in terms of the three metrics compared in our simulations.

VII. CONCLUSION

In this paper, the process of healthcare data communication is considered. We define the environment of hospital care as an incompletely predictable network (IPN), where nodes move in a limited range or with a certain trend. A novel protocol named the direction density-based secure routing protocol (DDSRP) is proposed to solve the transmission efficiency and communication security of healthcare data in IPNs. This protocol takes full advantage of the moving information of nodes to route in IPNs. Through the characteristics of IPNs, DDSRP utilizes the concept of direction density for routing with the information of nodes' moving direction and node group movement. Moreover, DDSRP ensures the security of healthcare data communication using an authenticated message transmission process. The simulation shows that the protocol performs well in terms of packet delivery ratio, normalized routing overhead and average end-to-end delay.

REFERENCES

[1] M. Ghamari, B. Janko, R. S. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A survey on wireless body area networks for ehealthcare systems in residential environments," *Sensors*, vol. 16, no. 6, p. 831, 2016.

[2] G. V. Crosby, T. Ghosh, R. Murimi, and C. A. Chin, "Wireless body area networks for healthcare: A survey," *Int. J. Ad Hoc, Sensor Ubiquitous Comput.*, vol. 3, no. 3, p. 1, 2012.

[3] M. Chen, Y. Zhang, Y. Li, M. M. Hassan, and A. Alamri, "AIWAC: Affective interaction through wearable computing and cloud technology," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 20–27, Feb. 2015.

[4] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 340–352, Feb. 2015.

[5] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2706–2716, Dec. 2016.

[6] T. Ma *et al.*, "Social network and tag sources based augmenting collaborative recommender system," *IEICE Trans. Inf. Syst.*, vol. E98.D, no. 4, pp. 902–910, 2015.

[7] M. Chen, Y. Ma, J. Song, C. F. Lai, and B. Hu, "Smart clothing: Connecting human with clouds and big data for sustainable health monitoring," *ACM/Springer Mobile Netw. Appl.*, vol. 21, no. 5, pp. 825–845, 2016.

[8] Y. Zhang, M. Chen, S. Mao, L. Hu, and V. Leung, "Cap: Crowd activity prediction based on big data analysis," *IEEE Netw.*, vol. 28, no. 4, pp. 52–57, Jul. 2014.

[9] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[10] A. Tewari and P. Verma, "Security and privacy in E-healthcare monitoring with WBAN: A critical review," *Int. J. Comput. Appl.*, vol. 136, no. 11, p. 1, 2016.

[11] G. E. de Andrade, L. A. de P. Lima, A. Calsavara, J. A. de Oliveira, and G. Michelon, "Message routing in vehicular delay-tolerant networks based on human behavior," in *Proc. 10th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Jul. 2016, pp. 1–6.

[12] J. Shen, S. Moh, I. Chung, and X. Sun, "Buffer scheme optimization of epidemic routing in delay tolerant networks," *J. Commun. Netw.*, vol. 16, no. 6, pp. 656–666, Dec. 2014.

[13] J. Shen, C. Wang, A. Wang, X. Sun, S. Moh, and P. C. Hung, "Organized topology based routing protocol in incompletely predictable ad-hoc networks," *Comput. Commun.*, to be published, doi: 10.1016/j.comcom.2016.07.009.

[14] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Inf. Syst.*, vol. 48, pp. 132–150, Mar. 2015.

[15] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. IEEE Workshop Mobile Comput. Syst. Apps*, vol. 6, no. 7, pp. 90–100, Jul. 1999.

[16] H. Abdulwahid, B. Dai, B. Huang, and Z. Chen, "Scheduled-links multicast routing protocol in MANETs," *J. Netw. Comput. Appl.*, vol. 63, pp. 56–67, Mar. 2016.

[17] J. Shen, S. Moh, and I. Chung, "A priority routing protocol based on location and moving direction in delay tolerant networks," *IEICE Trans. Inf. Syst.*, vol. 93, no. 10, pp. 2763–2775, 2010.

[18] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, and C. Youn, "Wearable 2.0: Enable human-cloud integration in next generation healthcare system," *IEEE Commun.*, vol. 54, no. 12, Dec. 2016.

[19] R. Kouah, S. Moussaoui, and M. Aissani, "Direction-based greedy forwarding in mobile wireless sensor networks," in *Proc. 8th Adv. Int. Conf. Telecommun.*, 2012, pp. 69–74.

[20] A. K. Gupta, I. Bhattacharya, P. S. Banerjee, J. K. Mandal, and A. Mukherjee, "Dirmove: Direction of movement based routing in DTN architecture for post-disaster scenario," *Wireless Netw.*, vol. 22, no. 3, pp. 723–740, 2016.

[21] K. Z. Ghafoor, J. Lloret, A. S. Sadiq, and M. A. Mohammed, "Improved geographical routing in vehicular ad hoc networks," *Wireless Pers. Commun.*, vol. 80, no. 2, pp. 785–804, 2015.

[22] K. Pandey, S. K. Raina, and R. S. Raw, "Distance and direction-based location aided multi-hop routing protocol for vehicular ad-hoc networks," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 16, no. 1, pp. 71–98, 2016.

[23] J. Y. Li and R. S. Ko, "Geographical model-derived grid-based directional routing for massively dense WSNS," *Eurasip J. Wireless Commun. Netw.*, vol. 2016, no. 1, pp. 1–22, 2016.

[24] S. P. Salunkhe and H. D. Patil, "Delay efficient authenticated anonymous secure routing for MANETs," *Int. J. Comput. Appl.*, vol. 148, no. 4, pp. 29–33, 2016.

[25] J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design," *J. Commun. Netw.*, vol. 14, no. 6, pp. 682–691, Dec. 2012.

[26] M. Sbeiti, N. Goddemeier, D. Behnke, and C. Wietfeld, "Paser: Secure and efficient routing approach for airborne mesh networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 1950–1964, Mar. 2016.

[27] T. A. Babbitt and B. K. Szymanski, "Trust based secure routing in delay tolerant networks," in *Proc. 8th IEEE Int. Workshop Netw. Sci. Commum. Netw. (NetSciCom)*, San Francisco, CA, USA, 2016, pp. 846–851.

[28] J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang, "An efficient and private RFID authentication protocol supporting ownership transfer," *J. Internet Technol.*, vol. 17, no. 3, p. 2, 2016.

[29] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: A fuzzy attribute-based signcryption scheme," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 37–46, Sep. 2013.

[30] J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. V. Vasilakos, "4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," *Inf. Sci.*, vol. 314, pp. 255–276, Sep. 2015.

[31] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, to be published, doi: 1 0.1109/JSYST.2016.2544805.

[32] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security," *ACM/Springer Mobile Netw. Appl.*, vol. 21, no. 5, pp. 729–743, 2016.

[33] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, "Secure routing based on social similarity in opportunistic networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 594–605, Jan. 2016.

[34] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, Feb. 2016.

[35] B. Luo, Y. Jin, S. Luo, and Z. Sun, "A symmetric lookup-based secure P2P routing algorithm," *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 5, pp. 2203–2217, 2016.

[36] A. Ahmed, K. A. Bakar, M. I. Channa, and A. W. Khan, "A secure routing protocol with trust and energy awareness for wireless sensor network," *Mobile Netw. Appl.*, vol. 21, no. 2, pp. 272–285, 2016.

[37] T. Wang, Y. Cao, Y. Zhou, and P. Li, "A survey on geographic routing protocols in delay/disruption tolerant networks," *Int. J. Distrib. Sensor Netw.*, vol. 2016, no. 6, pp. 1–12, Jan. 2016.

[38] S. K. Pasupuleti, S. Ramalingam, and R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," *J. Netw. Comput. Appl.*, vol. 64, pp. 12–22, Apr. 2016.

[39] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," *J. Internet Technol.*, vol. 16, no. 2, pp. 317–323, 2015.

[40] J. Shen, H. Tan, S. Moh, and I. Chung, "Enhanced secure sensor association and key management in wireless body area networks," *J. Commun. Netw.*, vol. 17, no. 5, pp. 453–462, 2015.

[41] G. S. Rao, E. Jagadeeswararao, U. J. Priyanka, and T. I. P. Darsini, "Performance analysis of MANET routing protocols-dsdv, DSR, AODV, AOMDV using NS-2," *Global J. Comput. Sci. Technol. (E)*, vol. 15, no. 6, pp. 1–11, 2015.

[42] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *J. Internet Technol.*, vol. 16, no. 1, pp. 171–178, 2015.

JIAN SHEN (M'11) received the B.E. degree from the Nanjing University of Information Science and Technology, Nanjing, China, in 2007, and the M.E. and Ph.D. degrees in computer science from Chosun University, Gwangju, South Korea, in 2009 and 2012, respectively. Since 2012, he has been a Full Professor with the School of Computer and Software, Nanjing University of Information Science and Technology. His research interests include computer networking, security systems, mobile computing and networking, ad hoc networks and systems, and ubiquitous sensor networks.

CHEN WANG received the B.E. degree from the Nanjing University of Information Science and Technology, Nanjing, China, where he is currently pursuing the M.E. degree. He focuses on information security and incompletely predictable ad hoc networks. His research interests include information security, ad hoc networks and systems, and wireless sensor networks.

CHIN-FENG LAI (SM'14) received the Ph.D. degree from the Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan, in 2008. He is currently an Associate Professor with the Department of Engineering Science, National Cheng Kung University. He has authored/co-authored over 100 refereed papers in journals, conferences, and workshop proceedings about his research areas within four years. His research interests include multimedia communications, sensor-based healthcare, and embedded systems. He is a member of the IEEE Circuits and Systems and the IEEE Communications Societies.

ANXI WANG received the B.E. degree from the Nanjing University of Information Science and Technology, Nanjing, China, where he is currently pursuing the M.E. degree. He focuses on energy efficient routing protocols in wireless sensor network and security systems. His research interests include ad-hoc networks and systems, information security, and wireless sensor networks.

HAN-CHIEH CHAO (SM'04) received the M.S. and Ph.D. degrees in electrical engineering from Purdue University in 1989 and 1993, respectively. Since 2010, he has been serving as the President of National Ilan University (NIU), Yilan City, Taiwan, where he is currently a joint appointed Distinguished Professor with the Department Computer Science and Information Engineering and Electronic Engineering. He is also a Full Professor of the Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan. He has authored or co-authored five books and has authored about 400 refereed professional research papers. His research interests include high speed networks, wireless networks, ipv6 based networks, digital creative arts, and e-Government and Digital Divide. He was an Officer of Award and Recognition for the IEEE Taipei Section from 2010 to 2012. He is a Fellow of IET (IEE).