International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Random Direction Based Model for Intrinsic Secrecy in Wireless Sensor Network

Ramesh L[1], Dr. A. Marimuthu[2]

[1]Research Scholar, PG and Research Department of Computer Science, Government Arts College, Coimbatore-18, India

[2]Associate Professor, PG and Research Department of Computer Science, Government Arts College, Coimbatore-18, India

Abstract: ***The ability to exchange secret information is critical to many commercial, governmental, and military networks. Wireless secrecy is essential for communication confidentiality, health privacy, public safety, information superiority, and economic advantage in the modern information society. Wireless security schemes have typically evolved from those developed for traditional wire line applications, these schemes do not consider physical properties of the wireless channels. To overcome these problems, this research work develops a foundation for design and analysis of wireless networks with secrecy provided by intrinsic properties such as node spatial distribution, wireless propagation medium, and aggregate network interference. Here consider bi-dimensional random mobility and use a random direction (RD) model for path selection in WSN to increase the secrecy level. Use a Random Direction (RD) mobility model, In the RD mobility model, each node alternates a movement phase and a pause phase; at the beginning of the movement phase, a node independently selects its new direction and speed, randomly selects a path during the data transmission phase to increase the secrecy level. Obtain the distance distribution function of any node pairs in a network, with node mobility based on the RD mobility model. Speed and direction are kept constant for the whole duration of the movement phase. In this model, nodes in WSN are uniformly distributed within the simulation area. Compared to the random waypoint (RWP) mobility model, it eliminates the phenomenon of clustering which occurs near the center of the simulation area. In this work, investigate the interference and SIR distribution functions of mobile nodes with a Random Direction (RD) at a given time instant t. The experimentation results shows that the intrinsic properties of wireless networks with Random Direction (RD) model can provide a new level of secrecy, paving the way to the design of wireless networks with enhanced intrinsic secrecy.***

Keywords: RD, Secrecy, SIR, Network interference

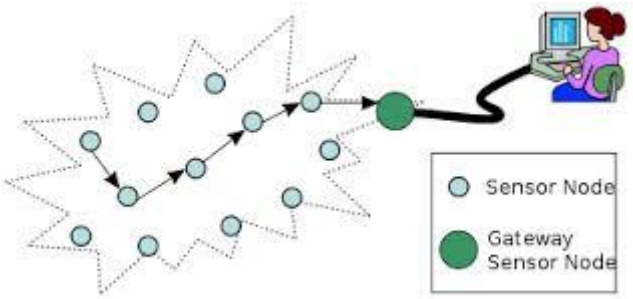
1. Introduction

A Wireless Sensor Network (WSN) is a group of specialized transducers with a communications infrastructure intended to monitor and record conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one or several sensors. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions



2. Architecture of Wireless Sensor Network

The architecture of WSN differs for each individual sensor micro module and depends on its entire network. Energy efficiency, size reduction and minimum cost are the main factors determine sensor micro module architecture. A wireless sensor micro module or micro module is also called as mote and consist of four functional components: sensing unit, processing unit, transceiver, and power unit. The structural block diagram of a sensor micro module is shown by the figure 1.1[1].

1) Sensing Unit
It consists of a consist of sensors that can measure the physical characteristics of its environment.

2) Processing Unit
A microcontroller processes information and controls the working of other parts in the sensor micro module. A microcontroller is should be less expensive, ease to attach other devices, simplicity of programming, and low power utilization.

3) Transceiver
Messages are sending and receive wirelessly by transceiver. Combination of transmitter and receiver into a single device is known as a transceiver. A transceiver must have an optimal balance between a low data rate and small energy consumptions.

4) Power source
Power source provide energy to all component of WSN. Changing the battery regularly can be expensive and problematic. Sensing, communicating and data processing need power consumption in sensor micro module. Communication of information needs more energy than any other process. The power stored in batteries or capacitors is main source of energy in sensor micro module. Solar sources, heat differences, or pulsation can be used to renew energy required for sensor.

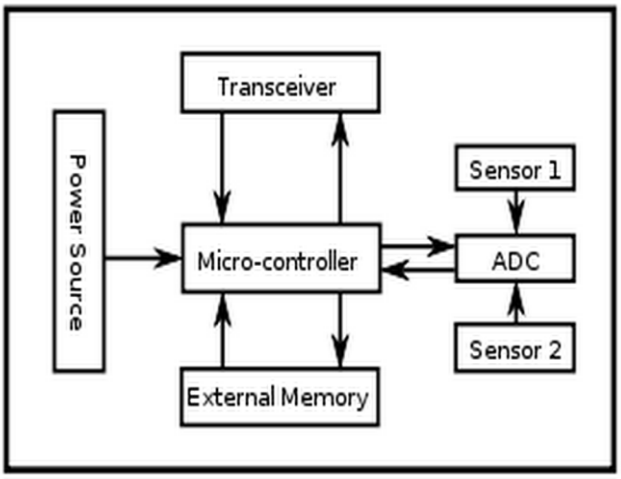


Figure 1.2: The typical architecture of the sensor node

3. Secrecy in Wireless Sensor Networks

Contemporary security systems for wireless networks are based on cryptographic primitives that generally ignore two key factors: (a) the physical properties of the wireless medium, and (b) the spatial configuration of both the legitimate and malicious nodes. These two factors are important since they affect the communication channels between the nodes, which in turn determine the fundamental secrecy limits of a wireless network. In fact, the inherent randomness of the wireless medium and the spatial location of the nodes can be leveraged to provide intrinsic security of the communications infrastructure at the physical-layer level.

The basis for information-theoretic security, which builds on the notion of perfect secrecy. More recently, there has been a renewed interest in information-theoretic security over wireless channels, from the perspective of space-time communications [1], multiple-input multiple-output communications [2]–[3], eavesdropper collusion [4-5], cooperative relay networks [6], fading channels [7]–[8], strong secrecy [9-10], secret key agreement [11]–[12], code design [13]–[14], among other topics comprehensive treatment of physical-layer security can be found in [15]. A fundamental limitation of the literature is that it only considers scenarios with a small number of nodes. To account for large-scale networks composed of multiple legitimate and eavesdropper nodes, secrecy graphs were introduced in [16] from a geometrical perspective, and in [17] from an information-theoretic perspective. The local connectivity of secrecy graphs was extensively characterized in [17], while the scaling laws of the secrecy capacity were presented in [18-19]. The feasibility of long-range secure communication was proved in [20], in the context of continuum percolation.

4. Existing System

Existing work establish foundations for the design and analysis of wireless networks with intrinsic secrecy. In particular, we develop a framework accounting for:

1) The spatial distributions of legitimate, eavesdropping, and interfering nodes;
2) The physical properties of the wireless propagation medium; and
3) The characteristics of aggregate network interference.

Recent approach is based on stochastic geometry, probability theory, and communication theory. The key contributions of the work can be summarized as follows:

Introduction of the concept of network secrecy and new metrics for characterizing intrinsic wireless secrecy in scenarios composed by legitimate, eavesdropping, and interfering nodes;

Development of a framework for design and analysis of wireless networks with intrinsic secrecy that accounts for node spatial distribution, physical propagation medium, and aggregate network interference;

Characterization of the received signal-to-interference ratios (SIRs) in legitimate and eavesdropping networks for different destination selection techniques; and

Quantification of the network secrecy performance provided by legitimate network strategies that mitigate the capabilities of the eavesdropping network.

4.1 Disadvantages

- Security in wireless systems is challenging due to the broadcast nature of the channel ,automatic selection of the key values
- Less secrecy when compare to random selection of the path to data transmission

5. Proposed System

The key contributions of the research work can be summarized as follows:

Introduction of the concept of network secrecy and new metrics for characterizing intrinsic wireless secrecy in scenarios composed by legitimate, eavesdropping, and interfering nodes;

Development of a framework for design and analysis of wireless networks with intrinsic secrecy that accounts for

node spatial distribution, physical propagation medium and aggregate network interference;

Characterization of the received Signal-To-Interference Ratios (SIRs) in legitimate and eavesdropping networks for different destination selection techniques; and • quantification of the network secrecy performance provided by legitimate network strategies that mitigate the capabilities of the eavesdropping network.

Here consider bi-dimensional random mobility and use a random direction (RD) mobility model. Use a Random Direction (RD) mobility model, In the RD mobility model, each node alternates a movement phase and a pause phase; at the beginning of the movement phase, a node independently selects its new direction and speed, randomly selects a path during the data transmission phase to increase the secrecy level. Obtain the distance distribution function of any node pairs in a network, with node mobility based on the RD mobility model. Speed and direction are kept constant for the whole duration of the movement phase.

In this model, nodes in WSN are uniformly distributed within the simulation area. Compared to the random waypoint (RWP) mobility model, it eliminates the phenomenon of clustering which occurs near the center of the simulation area. In this work, investigate the interference and SIR distribution functions of mobile nodes with a Random Direction (RD) at a given time instant *t*.

Propose an approximate expression for the interference and SIR distribution functions at a tagged node. However, if the tagged node moves, the distance between the tagged node and each interferer is not independent.

5.1 Advantages

Based on the probability distribution function of distance between any node pairs, theoretically estimate the distribution of the accumulated interference contributed by concurrent transmissions and the corresponding SIR values, which increases the secret level of the methods.

Investigate the probability of successful transmissions for measuring the network intrinsic secrecy in WSN.

6. Problem Objectives

The major objective of this research work is to propose a new schema to solve security problem in wireless systems regarding to broadcast nature of the channel, which facilitates the interception of radio communications.

The proposed work solves the wireless security problem in wire line applications; and additionally considers physical properties of the wireless channels.

The ability to exchange secret information between nodes inside the wireless networks becomes more secure for commercial, governmental, and military networks.

A fundamental issue arising in WSN is the increase the security, an optimal way to solve this problem is the selection of the optimal path between any two nodes. A method that has been advocated to improve routing efficiency is to select the most stable path so as to reduce the latency and the overhead due to route reconstruction.

6.1 Proposed Methodology

Development of a framework for design and analysis of wireless networks with intrinsic secrecy that accounts for node spatial distribution, physical propagation medium and aggregate network interference;

Characterization of the received Signal-To-Interference Ratios (SIRs) in legitimate and eavesdropping networks for different destination selection techniques; and • quantification of the network secrecy performance provided by legitimate network strategies that mitigate the capabilities of the eavesdropping network.

Here consider bi-dimensional random mobility and use a random direction (RD) mobility model. Use a Random Direction (RD) mobility model, In the RD mobility model, each node alternates a movement phase and a pause phase; at the beginning of the movement phase, a node independently selects its new direction and speed, randomly selects a path during the data transmission phase to increase the secrecy level. Obtain the distance distribution function of any node pairs in a network, with node mobility based on the RD mobility model. Speed and direction are kept constant for the whole duration of the movement phase.

In this model, nodes in WSN are uniformly distributed within the simulation area. Compared to the random waypoint (RWP) mobility model, it eliminates the phenomenon of clustering which occurs near the center of the simulation area. In this work, investigate the interference and SIR distribution functions of mobile nodes with a Random Direction (RD) at a given time instant *t*.

Propose an approximate expression for the interference and SIR distribution functions at a tagged node. However, if the tagged node moves, the distance between the tagged node and each interferer is not independent.

During this model , Let us consider two generic nodes, A and B, and let $X_A(t)$ and $X_B(t)$ be their positions, respectively, at time t. Define the distance between the two nodes at time t as: $d_{A,B}(t) = ||X_A(t) - X_B(t)||$. According to assumption (iii), a communication link between A and B exists if the two nodes are within the radio range of each other. Then, considering assumption (i), Link between A and B exists at time t if $d_{A,B}(t) < R$, and this link is bidirectional

Let us define the probability of link availability $A_{link}(d_{A;B}(0); t)$ as the probability that the link between nodes A and B is active at time t, given that the initial distance between the two nodes is equal to $d_{A,B}(0), 0 \leq d_{A,B}(0) < R$, i.e.,

$$A_{link}(d_{A,B}(0), t) = \mathbb{P}(d_{A,B}(0) < R \,|d_{A,B}(0))$$

Now, consider n+1 mobile nodes, and let Xi(t) be the position of node i with $1 \leq i \leq n+1$ at time t. Assume that $d_{i,i+1}(0) < R$ for $1 \leq i \leq n$ and let us denote by $d_0 = [d_{1,2}(0), .., d_{n,n+1}(0)]$ the vector of initial nodes distances $d_{i,i+1}(0), 1 \leq i \leq n$ Then, consider a path of n hops, obtained by visiting the n + 1 nodes in sequence: $1 \rightarrow 2 \rightarrow 3 \rightarrow \cdots \rightarrow n+1$. The probability of path availability at time t is defined as:

$$A_{path}(d_0, t) = \mathbb{P}(d_{i,i+1}(l) < R \forall i \leq n | d_0)$$

We define the link duration probability, $D_{link}(d_{A,B}(0),t)$, as the probability that the link between A and B has been uninterruptedly active till time t, given that their initial distance is $d_{A,B}(0)$, $0 \leq d_{A,B}(0) < R$.

$$D_{link}(d_{A,B}(0),t) = P(inf\{_T s.t.\ d_{A,B}(_T) > R\} > t | d_{A,B}(0))$$

while the path duration probability Dpath(d0; t) is the probability that the path has been uninterruptedly active till time t:

$$D_{path}(d_0, t) = \mathbb{P}(\inf(\tau\ st\ for\ some\ i, 1 \leq i \leq n, d_{i,i+1}(\tau) > R) > t | d_0)$$

Under the RD model [21], each node alternates a movement phase and a pause phase. At the beginning of the movement phase, a node independently selects its new direction and speed. The direction is uniformly distributed in a range from 0 to 2π and the speed is uniformly distributed in a range from 0 to V_{max}. The speed and direction are kept constant for the whole duration of the movement phase. The durations of movement and pause phases follow an exponentially distributed with parameters λ and μ, respectively. Its speed keeps constant during each segment but varies uniformly on $[V_{min}, V_{max}]$ at endpoints. The endpoints of RD must be on the boundary, which is to say that nodes cannot stop in the middle of the region apply geometric probability to analyze node distribution of RD model. In the case of circular regions, a closed form node distribution is obtained. Furthermore, analyze the speed distribution of RD by the method of palm calculus and give a general explanation to the hypostasis of speed decay phenomenon. At last, it should be noted that the appellation "random direction model" is also used to emulate Brownian motions.

In the first case, extract the node trajectories as the sum of random phasor. At this point the Central Limit Theorem cannot be directly applied. However, the phasor could be decomposed into the horizontal and vertical components, and the sum of the horizontal and vertical components closely follows a normal distribution.

Consider the Random Direction model (RD) i.e., each node alternates periods of movement (*move* phase) to periods during which it pauses (*pause* phase); at the beginning of each *move* phase, a node independently selects its new direction and speed of movement. Speed and direction are kept constant for the whole duration of the node *move* phase; the durations of *move* and *pause* phases are, in general, distributed according to independent random variables.

Under the RD model, the temporal evolution of the node position, either in the *move* or in the *pause* phase, can be described through a system of partial differential equations (PDE's) [22]. In [22], (weak) solution of the these equations have been obtained over a finite rectangular area. Here, instead, consider the dynamics of nodes moving over an infinite bidimensional domain, and obtain a closed expression for the general (weak) solution of the RD equations in the frequency domain (i.e., the moment generating function), under the assumption that *move* and *pause* times are exponentially distributed. Even if a direct analytical inverse transform of the obtained moment generating function appears to be prohibitive, closed expressions for the moments of the spatial Probability Density Function (PDF) can easily be derived. By using the node spatial distribution, write an exact expression for the probability of link availability, and then propose a simple approximation to evaluate this metric based on the second moment of the spatial distribution, which provides satisfactory results.

7. Conclusion

In this paper have the methodology and way regarding to find out the thing throughput, end to end delay, and packet delivery ratio and performance evaluation with the help of the proposed system, which is discussed in above chapters

References

[1] A. Hero, "Secure space-time communication," IEEE Transactions on Information, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
[2] R. Negi and S. Goel, "Secret communication using artificial noise," in Proc. IEEE Vehicular Technology Conference, vol. 3, Dallas, TX, Sept. 2005, pp. 1906–1910.
[3] H. Weingarten, T. Liu, S. Shamai, Y. Steinberg, and P. Viswanath, "The capacity region of the degraded multiple-input multiple-output compound broadcast channel," IEEE Trans. Inf. Theory, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.
[4] L. Zhang, R. Zhang, Y. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," in Proc. Allerton Conf. on Communications, Control, and Computing, Monticello, IL, Sept. 2009.
[5] P. C. Pinto, J. O. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in Proc. IEEE Int. Symp. on Inf. Theory, Seoul, South Korea, July 2009, pp. 2442–2446.
[6] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," in Proc. IEEE Int. Symp. on Inf. Theory, Toronto, ON, July 2008, pp. 2217–2221.
[7] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in Proc. IEEE Int. Symp. on Inf. Theory, Adelaide, Australia, Sept. 2005, pp. 2152–2155.
[8] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, pp. 2470–2492, June 2008.
[9] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," Eurocrypt 2000, Lecture Notes in Computer Science, vol. 1807, pp. 351+, 2000.

[10] J. Barros and M. Bloch, "Strong secrecy for wireless channels," in Proc. International Conf. on Inf. Theor. Security, Calgary, Canada, Aug. 2008.
[11] U. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733–742, May 1993.
[12] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, "LDPCbased secret key agreement over the gaussian wiretap channel," in Proc. IEEE Int. Symp. on Inf. Theory, Seattle, USA, 2006.
[13] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
[14] J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," IEICE Trans. on Fund. Of Elec. Comm. Comp., vol. E89-A, no. 7, pp. 2036–2046, July 2006.
[15] M. Bloch and J. O. Barros, Physical-Layer Security. Cambridge University Press, 2011.
[16] M. Haenggi, "The secrecy graph and some of its properties," in Proc. IEEE Int. Symp. on Inf. Theory, Toronto, Canada, July 2008.
[17] P. C. Pinto, J. O. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in Proc. IEEE Int. Conf. on Commun. Systems, Guangzhou, China, Nov. 2008, pp. 974–979.
[18] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in Proc. IEEE Int. Symp. on Inf. Theory, June 2009, pp. 1189–1193.
[19] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," in Inf. Theory and Applications Workshop, San Diego, CA, Feb. 2010, pp. 1–4.
[20] P. C. Pinto and M. Z. Win, "Continuum percolation in the intrinsically secure communications graph," in Proc. IEEE Int. Symp. on Inf. Theory and Its Applications, Taichung, Taiwan, Oct. 2010, pp. 1–6.
[21] P. Nain, D. Towsley, B. Liu, and Z. Liu, "Properties of Random Direction Models," in Proc. IEEE INFOCOM, pp. 1897-1907, Mar. 2005.
[22] M. Garetto and E. Leonardi, "Analysis of Random Mobility Models with PDEs, in Proc. ACM MobiHoc, pp. 73-84, May 2006.

Author Profile

L. Ramesh received the B.Sc (CS) and M.Sc (CS) Degrees from Bharathiar University, Coimbatore, Tamilnadu, India, in 2012 and 2014 respectively, currently he doing his research in a broad field of Network security in Government Arts College, Coimbatore.

Dr. A. Marimuthu M.C.A., M.Phil., M.B.A (Systems)., Ph.D.., received his UG and PG Degree from Gobi Arts and Science college, Bharathiar University, Tamilnadu, India. Received his M.B.A (Systems) Degree from Periyar University, Salem, India. Received his Ph.D Degree from Vinayaga Mission University, India. He had 20 years of teaching experience and 10 years of Research experience. He has attended, presented and published more than 20 research paper in various national and international conferences and journals. Professional activities include guided various projects for M.C.A, M.Sc Computer Science and M.Sc Information Technology Students. He has produced 15 M.Phil Scholars. Currently eight Ph.D scholars are pursuing their research program in Computer Science under his Supervision.