ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Data Transfer through Secured Routing Model in WSN

Aiswarya P.S [1], Ms.K.Sindhuja[2]

P.G. Student, Department of Computer Science and Engineering, Easa College of Engineering and Technology, Coimbatore, India[1]

Assistant Professor, Department of Computer Science and Engineering, Easa College of Engineering and Technology, Coimbatore, India[2]

ABSTRACT: Wireless sensor networks (WSNs) nowadays considered as a hot research topic because of its wide range of applications in various fields. Recently, advancement in network communications has led to multi-purpose sensor nodes with low-cost and power consumption. Wireless sensor networks are composed of limited power which their power supply could not be replaced or recharged. So, less power consumption will increase the lifetime of these networks. Therefore, providing efficient routing algorithms with less energy consumption is desirable. Among many routing algorithms, approaches based on clustering, result less energy consumption. The scheme reduces intra cluster communication distance and hence increases the energy efficiency. Multiple-path source routing protocols allow a data source node to distribute the total traffic among available paths. I consider the problem of jamming-aware source routing in which the source node performs traffic allocation based on observed jamming statistics at individual network nodes. I formulate this traffic allocation as a lossy network flow optimization problem using portfolio selection theory from financial statistics. I show that in multi-source networks, this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network service maximization (NSM). I demonstrate the network's ability to estimate the impact of jamming and incorporate these estimates into the traffic allocation problem. Finally, I simulate the achievable throughput using our proposed traffic allocation method in several scenarios

KEYWORDS*:* Wireless communication, energy-aware systems,routing protocols.

I. INTRODUCTION

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. 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 cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

II. LITERATURE SURVEY

1. Energy And Link-State Based Routing Protocol For Manet

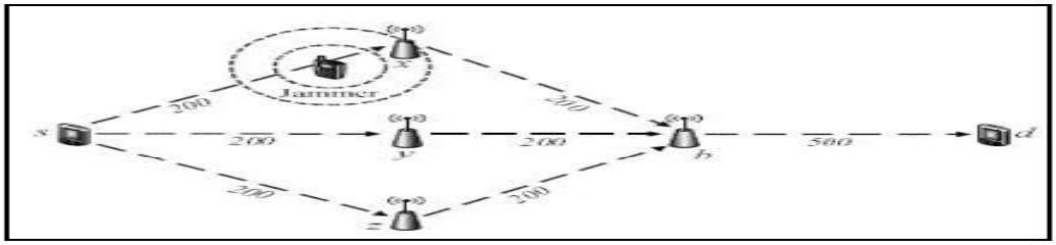
A mobile ad hoc network is a mobile, multihop wireless network that does not rely on any preexisting infrastructure. Mobile ad hoc networks are characterized by dynamic topologies due to uncontrolled node mobility, limited and variable shared wireless channel bandwidth, and wireless devices constrained by battery power. One of the key challenges in such networks is to design dynamic routing protocols that are efficient, that is, consume less overhead the goal of minimizing the routing overhead. These protocols reactively discover and maintain only the needed routes, in contrast to proactive protocols which maintain all routes regardless of their usage. The key characteristic of an on-demand protocol is the source-initiated route discovery procedure. frequency low.

2. Multipath Routing Mechanism With Load Balancing In Ad Hoc Network

Mobile Ad hoc Networks (MANET) are wireless networks consisting of a collection of mobile nodes with no fixed infrastructure. Due to their decentralized, self-configuring and dynamic nature, MANETs offer many advantages and are easy to install. But with this dynamic topology, mobile ad hoc networks have some challenges like the design of an efficient routing protocol. An example for this challenge is load balancing. The multipath routing protocol with load balancing provides a solution for the congestion network and increases it's capacity. To consider that the use of multiple paths simultaneously for transmission data allows to improve the network performance, i propose a new protocol LB-AOMDV (Load Balancing-AOMDV), a solution to achieve better load balancing mechanism. The simulation's result shows the significant performance improvement of the network for the multipath routing protocol with load balancing. The proposed solution LB-AOMDV works better than other protocols in terms of average delay, capacity and load balance.

III. PROPOSED METHODOLOGY AND DISCUSSION

It will become apparent that the proposed algorithms apply in a more general environment, relying only on the measured Multipath Routing at each of the nodes in the network and being agnostic of the manner in which that Multipath Routing was generated and the geographical locations of the routers (i.e. the solution easily addresses routers with directional antennas, etc.). I will consider both static routers, which transmit the Multipath Routing signal continuously, and simple dynamic routers that switch randomly between transmitting the Multipath Routing signal and sleeping mode.



IV. SYSTEM MODEL

Security Mechanisms

Many security mechanisms have been proposed for the security of the WSN. Most of the mechanisms for the detection of the malicious nodes are based on the cryptography. The technique requires security keys in the algorithm that consume the memory storage space inside the device. There are different challenges in providing security to a WSN deployment. These are: There is a conflicting interest between minimization of resource consumption and maximization of security level. A better solution actually gives a good compromise between the two of them. During the design of any security solution I need to take care of following node resource limitations like memory and energy, sensor network constraints like unreliable communication, collisions and latency and physical limitation like unattended after deployment and remotely managed. The type of security mechanism that can be hosted on a sensor node platform is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

dependent on the capabilities and limitations or constraints of sensor node hardware. Ad-hoc networking topology of WSN facilitates attackers for different types of link attacks ranging from passive eavesdropping to active interfering. Attacks on a WSN can come from all directions and target at any node leading to leaking of secret information, interfering message, the communication in WSN is through wireless media, mainly radio. This characteristic of WSN makes wire-based security schemes impractical for WSNs. The topology of WSN is always dynamic. The sensor nodes can come and go in an arbitrary fashion. Node failures may be permanent or intermittent and this gives a higher level of system dynamics. Again very often large numbers of nodes are expected in sensor network deployments and the nature of it is unpredictable. The problem of detecting the malicious nodes has been addressed separately in different protocols, which are either extensions or based on secure routing protocols.

Threat For Wireless Networks

The effectiveness and simple implementation of physical layer jammers make them an essential threat for wireless networks. In a multi hop wireless network, where jammers can interfere with the transmission of user messages at intermediate nodes along the path, one can employ jamming oblivious routing and then employ physical-layer techniques (e.g. spread spectrum) to suppress jamming.

Due to their broadcast nature, wireless networks are susceptible to many security attacks. Among them, denial-of-service (DoS) attacks can severely disrupt network performance, and thus are of interest here. In particular, jamming the physical layer is one of the simplest and most effective attacks, as any cheap radio device can broadcast electromagnetic radiation to block the communication channel.

Signal-To-Noise Ratio

Jamming in wireless networks is defined as the disruption of existing wireless communications by decreasing the signal-to-noise ratio at receiver sides through the transmission of interfering wireless signals. Jamming is different from regular network interferences because it describes the deliberate use of wireless signals in an attempt to disrupt communications whereas interference refer to unintentional forms of disruptions. Unintentional interference may be caused by the wireless communications among nodes within the same networks or other devices (e.g. microwave and remote controller). On the other hand, intentional interference is usually conducted by an attacker who intends to interrupt or prevent communications in networks. Jamming can be done at different levels, from hindering transmission to distorting packets in legitimate communications.

A straightforward approach to combat adversaries that jam transmissions in the network, particularly in a system with transmitters and receivers capable of operating over a large bandwidth, is to employ physical-layer mitigation techniques. Prominent among these approaches are direct-sequence and frequency-hopped spread spectrum, each of which employs a significantly larger bandwidth than that required for message transmission in order to allow for interference suppression. These techniques allow a significant reduction in the impact of the interference, often on the order of the ratio of the system bandwidth to the data rate

Routing Approaches Adversarial Jammers

This motivates the consideration of routing approaches to avoid adversarial jammers if it can be justified from the perspective of minimizing total cost to the network. In this work, I consider wireless communication between a source and a destination in a multi-hop fashion in the presence of multiple physical layer jammers that are spread over the network area at arbitrary locations by the adversary. I define that cost to be the aggregate energy expended by the system nodes to reliably transmit a message from the source to the destination, with reliability measured by an outage constraint.

Specifically routing algorithms in the presence of multiple jammers are investigated, but the energy consumption of the network nodes is not considered. Excessive energy consumption quickly depletes battery-powered nodes, and causes increased interference, resulting in a lower network throughput; thus, it is essential to seek methods to reduce energy consumption of the network nodes.

Each sensor node synchronizes to a reference node by using time information flooded by this node, as well as synchronizes to its neighboring nodes by employing the agreement algorithm.

NSM is a completely decentralized protocol since each sensor node synchronizes to its neighboring nodes and there is not any special node which acts as a time reference. For the evaluation of these protocols, I focused on the instantaneous global skew and local skew between sensor nodes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

System Model

I consider a wireless network where the system nodes are located arbitrarily. Let G = (N;L) denote the graph of the network where N denotes the set of network nodes and L denotes the set of links between them (a link can be potentially formed between any pair of nodes in the network).

In addition, malicious jammers are present in the network at arbitrary locations, and these jammers try to interfere with the transmission of the system nodes by transmitting random signals.

I assume that each jammer utilizes an omni directional antenna and can transmit over the entire frequency band; thus, spread spectrum or frequency hopping strategies improve performance via the processing gain, but are not completely effective in interference suppression.

One of the system nodes (source) chooses relays, with which it conveys its message to the destination in a (possibly)multi-hop fashion. Suppose the relays that the source selects construct a K-hop route between the source and the destination.

A K-hop route ∏ is determined by a set of K links ∏ = { l1,…,lk}and K + 1 nodes (including source and destination) such that link `k connects the kth link transmitter Sk to the kth link receiver Dk.

I denote the set of jammers by J and consider both static jammers and dynamic jammers. In the case of static jammers, each jammer transmits white Gaussian noise with a fixed power.

Since the jammers are active, assume initially that the transmit power and the location of jammers are known to the system nodes; In my proposed method, the knowledge of the transmit powers and locations of jammers is not necessary; in fact, the system nodes can measure the average received jamming (averaged over the multipath fading) and use this estimate of jamming interference for efficient routing.

In the case of dynamic jammers, each jammer switches between an “ON” state, when it transmits the jamming signal, and an “OFF” state or sleeping mode randomly and independently from the other jammers. These dynamic jammers are especially useful when the battery life of the jammers is limited and the adversary tries to cover a larger area, as the jammers in sleep mode can save significant energy.

I assume frequency non-selective Rayleigh fading between any pair of nodes. For instance, for link k between nodes Sk and Dk, let hk denote the fading, and {hj, k }j ∈ J denote the respective fading coefficients between jammers and Dk. It follows that the channel fading power is exponentially distributed. Without loss of generality, assume E[|hk|2] = 1; ∀ k, and E[|hk|2] = 1; ∀ j, k, and then work path-loss explicitly into (1) below. Also, each receiver experiences additive white Gaussian noise with power N0. Hence, the signal received by node Dk from node Sk is

$$y^{(k)} = \frac{h_k\sqrt{P_k}}{d_k^{\alpha/2}}x^{(k)} + \sum_{j\in\mathcal{J}}\frac{h_{j,k}\sqrt{P_j}}{d_{j,k}^{\alpha/2}}x^{(j)} + n^{(k)},$$

(1) where Pk is the transmit power of node Sk, Pj is the transmit power of the jammer, dk is the distance between Sk and Dk, dj;k is the distance between j-th jammer and Dk, and ∏ is the path-loss exponent. Also, x(k) and x(j) are the unit power signals transmitted by Sk and j-th jammer.

If spread spectrum were employed, the model would obviously change to include the processing gain and further averaging of the fading, but the design process would be similar.

The wireless network of interest can be represented by a directed graph g={N,E}. the vertex set n represents the network nodes, and an ordered pair {i,j} of node is in the edges at E. if and only if node j can receive packets directly from node i. Assume that all communication is uncast over the directed edges in E. i.e each packet transmitted by node I €N is intended for a unique node j€N wih (i,j) €E.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

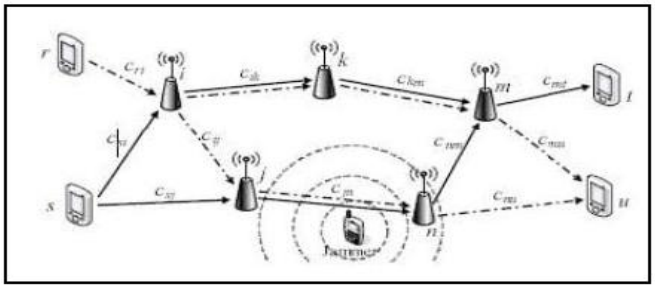


Fig. 1: An Example Network with Sources S = {r, s} Illustrated. Each Unicast Link (i; j) € E is Labeled with the Corresponding Link Capacity.

let Ps ={ps1; : : : ; psLs} denote the collection of Ls loop-free routing paths of the graph G. Figure 1 illustrates an example network with sources S= {r, s }.

The subgraph Gr consists of the two routing paths pr1 = {(r, i), (i, k), (k, m), (m, u)} pr2 = {(r, i), (i, j), (j, n), (n, u)}, and the subgraph Gs consists of the two routing paths ps1 = {(s, i), (i, k), (k, m), (m, t)} ps2 = {(s, j), (j, n), (n, m), (m, t)}.
. In order for a source node s to incorporate the jamming impact in the traffic allocation problem, the effect of jamming on transmissions over each link (i; j) ε Es must be estimated and relayed to sij Fig. 2, illustrates a single-source network with three routing paths

p1 = {(s; x); (x; b); (b; d)},
p2 = {(s; y); (y; b); (b; d)} and
p3 = {(s; z); (z; b); (b; d)}.

Each unicast link (i; j) is labelled with the corresponding link capacity cij in units of packets per second.

The proximity of the jammer to nodes x and y impedes packet delivery over the corresponding paths, and the jammer mobility affects the allocation of traffic to the three paths as a function of time.

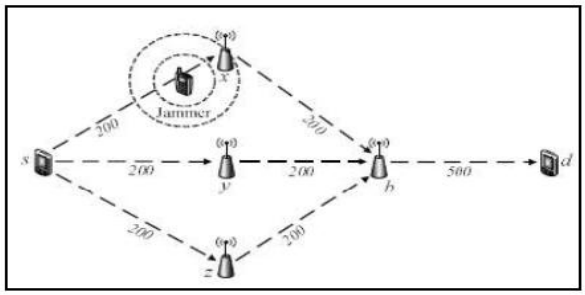


Fig. 2: An Example Network that Illustrates a Single-Source Network With three Routing Paths

The label on each edge (i; j) is the link capacity cij indicating the maximum number of packets per second (pkts/s) which can be transported over the wireless link. In this example, I assume that the source is generating data at a rate of 300 pkts/s. In the absence of jamming, the source can continuously send 100 pkts/sover each of the three paths, yielding a throughput rate equal to the source generation rate of 300 pkts/s. If a jammer near node xis transmitting at high power, the probability of successful packet reception, referred to as the packet success rate, over the link (s;x) drops to nearly zero, and the traffic flow to node d reduces to200 pkts/s. If the source node becomes aware of this effect, the allocation of traffic can be changed to 150 pkts/s on each of paths p2 and p3, thus recovering from the jamming attack at node X. Estimating Local Packet Success

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Rates xij (t) denote the packet success rate over link (i; j) € E at time t, noting that x(ij) (t)can be computed analytically as a function of the transmitted signal power of node i, the signal power of the jammers, I suppose that each node j maintains an estimate µij (t) of the packet success rate xij (t) as well as a variance parameter ε ij (t) to characterize both the uncertainty in the estimate and the variability in the process xij (t).

$$PDR_{ij}([t-T,t]) = \frac{v_{ij}([t-T,t])}{r_{ij}([t-T,t])}$$

This PDR can be used to update the estimate µij (t) at the end of the update period. In order to prevent significant variation in the estimate µij (t) I suggest using an exponential weighted moving average (EWMA) to update the estimate µj (t) as a function of the previous estimate µij (t - T)as

$$\mu_{ij}(t) = \alpha\mu_{ij}(t-T) + (1-\alpha)PDR_{ij}([t-T,t])$$

Optimal Jamming-Aware Traffic Allocation

In this section, I present an optimization framework for jamming aware traffic allocation to multiple routing paths in Ps for each source node s ε S. I develop a set of constraints imposed on traffic allocation solutions and then formulate a utility function for optimal traffic allocation by mapping the problem to that of portfolio selection in finance.

Traffic Allocation Constraints

In order to done a set of constraints for the multiple-path traffic allocation problem, consider the source data rate constraints, the link capacity constraints, and the reduction of traffic flow due to jamming at intermediate nodes The capacity constraint on the total traffic traversing a link (i,j) thus imposes the stochastic constraint

$$\sum_{s\in\mathcal{S}} \sum_{\ell:(i,j)\in p_{s\ell}} \phi_{s\ell} y_{s\ell}^{(i)} \le c_{ij}$$

let Ws denote the €xLs weighted link-path incidence matrix for source s with rows indexed by links (i, j) and columns indexed by paths p. The element w((i,j);,psl) in row (i; j) and column psl of Ws is thus given b

$$w((i,j),p_{s\ell}) = \begin{cases} \min\left\{1, \gamma_{s\ell}^{(i)} + \delta\omega_{s\ell}^{(i)}\right\}, & \text{if } (i,j) \in p_{s\ell} \\ 0, & \text{otherwise.} \end{cases}$$

Letting c denote the |€|x1 vector of link capacities cij for (i,j) ε E, the link capacity constraint can be expressed by the vector Inequality.

$$\sum \boldsymbol{W}_s \boldsymbol{\phi}_s \le \boldsymbol{c},$$

Optimal Traffic Allocation Using Portfolio Selection Theory
In order to determine the optimal allocation of traffic to the paths in Ps, each source s chooses a utility function I describe the desired analogy by mapping this allocation offends to financial assets to the allocation of traffic to routing paths. The analogy between financial portfolio selection and the allocation of traffic to routing paths is summarized below

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Portfolio Selection	Traffic Allocation
Funds to be invested	Source data rate R_s
Financial assets	Routing paths $\mathcal{P}_s$
Expected Asset return	Expected Packet success rate $\gamma_{s\ell}$
Investment portfolio	Traffic allocation ϕ_s
Portfolio return	Mean throughput $\gamma_s^T \phi_s$
Portfolio risk	Estimation variance $\phi_s^T \Omega_s \phi_s$

Optimal Jamming-Aware Traffic Allocation

$$\phi^* = \arg\max_{\{\phi_s\}} \sum_{s\in\mathcal{S}} \gamma_s^T \phi_s - k_s \phi_s^T \Omega_s \phi_s$$

$$\text{s.t.} \quad \sum_{s\in\mathcal{S}} W_s \phi_s \le c$$

$$1^T \phi_s \le R_s \text{ for all } s \in \mathcal{S},$$

$$0 \le \phi_s \text{ for all } s \in \mathcal{S}.$$

Optimal Distributed Traffic Allocation using NUM In the distributed formulation of the algorithm, each source determines its own traffic allocations, ideally with minimal message passing between sources. By inspection

Distributed Jamming-Aware Traffic Allocation

Initialize $n = 1$ with initial link prices λ_1.

1. Each source s independently computes
$$\phi^*_{s,n} = \arg\max_{\phi_s \in \Phi_s} \left(\gamma_s^T - \lambda_n^T W_s\right) \phi_s - k_s \phi_s^T \Omega_s \phi_s.$$
2. Sources exchange the link usage vectors
$u_{s,n} = W_s \phi^*_{s,n}$.
3. Each source locally updates link prices as
$$\lambda_{n+1} = \left(\lambda_n - a\left(c - \sum_{s\in\mathcal{S}} u_{s,n}\right)\right)^+.$$
4. If $\|\phi^*_{s,n} - \phi^*_{s,n-1}\| > c$ for any s, increment n and go to step 1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

VI. RESULTS

Source Node

This screenshot shows the starting node

Fig 3: Source Node

Packet Transfer

This screenshots shows the transferring of packet

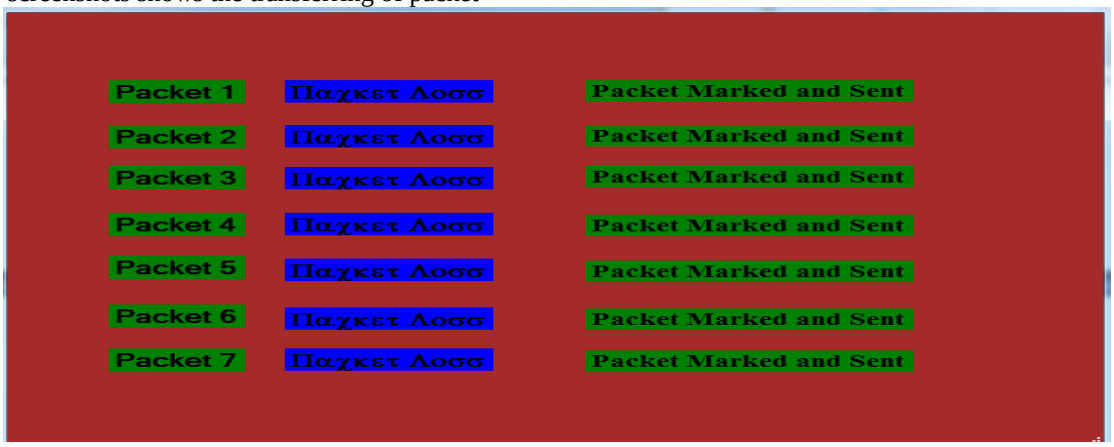


Fig 4: Packet Transfer

Transferring

This view shows the node transferring from source to destination

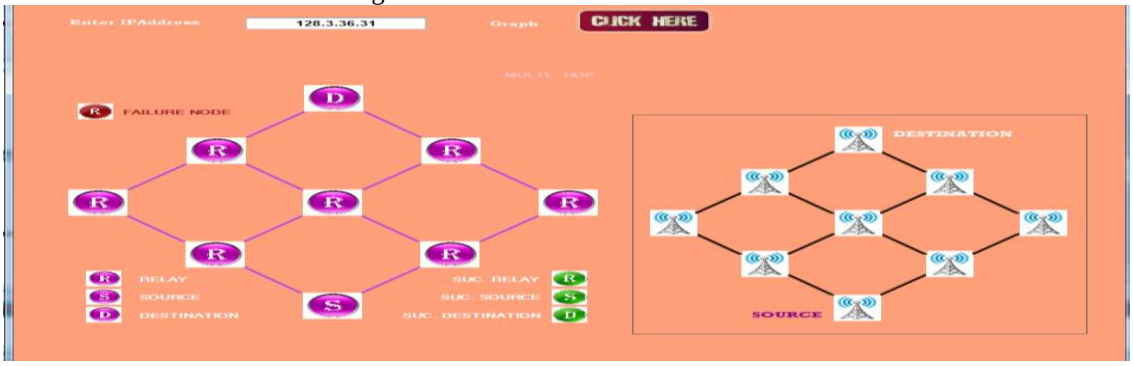


Fig 5: Transferring

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

File Processing Route

This screenshot shows the processing of file

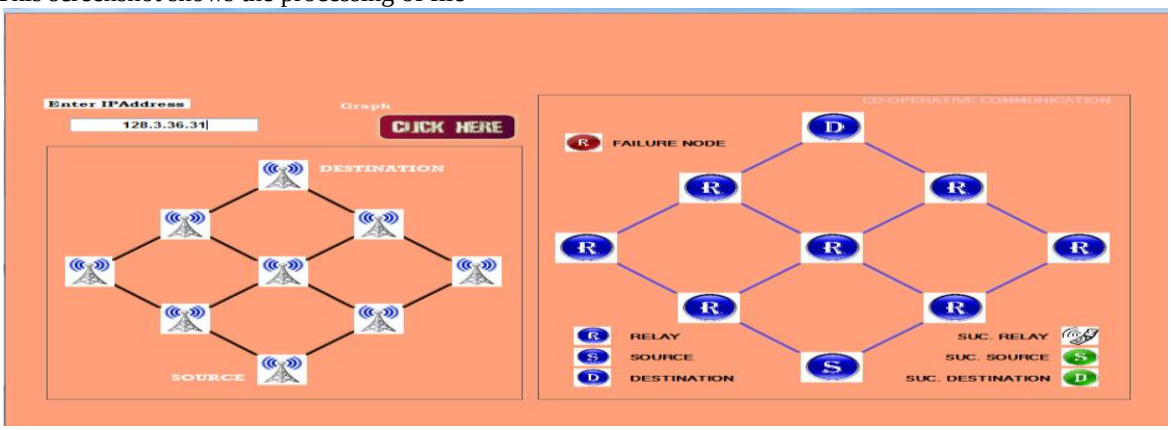


Fig 6: File Processing Route

Destination

This view shows the destination node

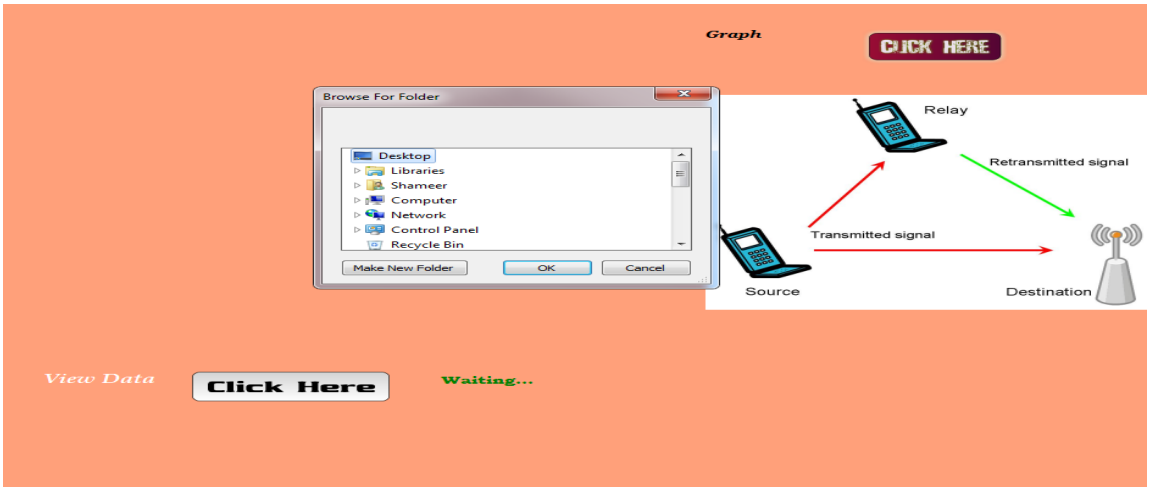


Fig 7: Destination node

VII. CONCLUSION AND FUTURE WORK

In this article, I studied the problem of traffic allocation in multiple-path routing algorithms in the presence of jammers whose effect can only be characterized statistically. I have presented methods for each network node to probabilistically characterize the local impact of a dynamic jamming attack and for data sources to incorporate this information into the routing algorithm. I formulated multiple-path traffic allocation in multi-source networks as a loss network flow optimization problem using an objective function based on portfolio selection theory from finance. I showed that this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization. I presented simulation results to illustrate the impact of jamming dynamics and mobility on network throughput and to demonstrate the efficiency of our traffic allocation algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

REFERENCES

[1] T. Y. Wu and C. H. Lin, "Low-SAR path discovery by particle swarm optimization algorithm in wireless body area networks," IEEE Sensors J., vol. 15, no. 2, pp. 928–936, Feb. 2015.
[2] C. Yi, L. Wang, and Y. Li, "Energy efficient transmission approach for WBAN based on threshold distance," IEEE Sensors J., vol. 15, no. 9, pp. 5133–5141, Sep. 2015.
[3] J. He, Y. Geng, Y. Wan, S. Li, and K. Pahlavan, "A cyber physical test-bed for virtualization of RF access environment for body sensor network," IEEE Sensors J., vol. 13, no. 10, pp. 3826–3836, Oct. 2013.
[4] D. Liu, Y. Geng, G. Liu, M. Zhou, and K. Pahlavan, "WBANs-Spa: An energy efficient relay algorithm for wireless capsule endoscopy," in Proc. IEEE 82nd Veh. Technol. Conf. (VTC-Fall), Boston, MA, USA, Sep. 2015, pp. 1–5.
[5] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," IEEE J. Biomed. Health Inform., vol. 18, no. 1, pp. 316–326, Jan. 2014.
[6] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1658–1686, Jan. 2014.
[7] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Commun., vol. 17, no. 1, pp. 51–58, Feb. 2010.
[8] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Secur. Privacy (HotWiSec), Budapest, Hungary, 2013, pp. 31–35.
[9] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
[10] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 3, pp. 614–624, Mar. 2013.
[11] H. Zhao, J. Qin, and J. Hu, "An energy efficient key management scheme for body sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2202–2210, Nov. 2013.
[12] D. He, S. Chan, Y. Zhang, and H. Yang, "Lightweight and confi- dential data discovery and dissemination for wireless body area networks," IEEE J. Biomed. Health Inform., vol. 18, no. 2, pp. 440–448, Mar. 2014.
[13] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-Lite: A lightweight identity-based cryptography for body sensor networks," IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 6, pp. 926–932, Nov. 2009.
[14] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.
[15] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 332–342, Feb. 2014.
[16] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 2894. New York, NY, USA: Springer-Verlag, 2003, pp. 452–474.
[17] G. Cagalaban and S. Kim, "Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption," in Proc. 13th Int. Conf. Adv. Commun. Technol. (ICACT), Seoul, Korea, Feb. 2011, pp. 863–867.