ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 2, Special Issue 12, April 2016.

Secure Scalable Traffic Allocation System in Wireless Environment using Multipath Routing System

Mrs.M.Abinaya[1], Ms.R.Bhuvaneshwari[2], Ms.P.Susmitha[3], Ms.P.Thiruselvi[4]

[1]Final year M.E(CSE), University College of Engineering, BIT Campus, Trichy
[2 3 4]Final Year B.Tech(IT), Sri Bharathi Engineering College for Women, Pudukkottai

Jamming attacks are especially harmful to the reliability of wireless communication, as they can effectively disrupt communication between any node pairs. Existing jamming defences primarily focus on repairing connectivity between adjacent nodes. In this work, to address new approach called Multipath Routing. Multipath routing protocol allows data source node to distribute the traffic data among available paths. This system considers the problem of jamming in which source node performs traffic allocation based on individual network nodes. In this proposed work using Dynamic Source Routing protocol (DSR) in a multi hop wireless adhoc networks f mobile nodes.DSR allows the network to self organizing and self configuring without need for any network infrastructure or administration. For the security purpose here uses Gaussian Random Key generation method to generate the key using user's information to encrypt with every pocket. The experimental results shows effectively and efficiently transfer the data from source and destination without jamming occurred.

Keywords: Dynamic Source Routing, Energy Aware multipath routing, Gaussian Random Key, Multipath routing.

I. INTRODUCTION

Non-Cooperative wireless networks have been received much attention in recent years, due to the fast advancement of mobile communication and P2P computing. Such a network can be formed by numerous heterogeneous personal mobile devices, such as laptops, tablets, smart phones, and so on. Because these devices are owned by different individuals, their behaviour might deviate from the norm due to various reasons.

Early designs of networking protocols often assume that a network consists of altruistic nodes that always follow the protocols, and thus mainly focus on handling exceptions due to other communication issues, such as transmission delay and packet loss. These designs tend to be less effective in non-cooperative networks, where there is no guarantee that selfish and malicious nodes obey the rules. A selfish player is also called rational in game theory literature, whose intention is to maximize its own utility. A malicious player is referred to be Byzantine in distributed computing literature, which deliberately deviates from the protocols to disrupt the normal operation of a network. Protocol design becomes quite challenging with the involvement of both rational and Byzantine behaviour in the same network.

In this work, focus on multi-path routing and forwarding in non-cooperative wireless networks, where nodes rely on each other to forward packets to the destination. Sending packets via multiple paths provide benefits such as route resilience, interference avoidance, and load/energy balancing. In the literature, two major approaches are developed for handling routing misbehaviour, either incentivizing nodes to cooperate, or punishing nodes that refuse to collaborate. Both approaches essentially treat selfish and malicious behaviours non-discriminatingly.

However, understand that neither approach is adequate to effectively deal with both kinds of misbehaviour. No incentive-based approach could encourage Byzantine nodes to cooperate, as they are not interested in their utility. On the other hand, to force rational nodes to cooperate via some punishment-based approaches is not reasonable in many cases. For example, if a rational node has already been overloaded or its battery level has dropped below a critical level, forcing it to cooperate certainly degrades the service quality and brings in potential loss. Therefore, separate the two kinds of misbehaviour and treat them accordingly.

Here it adapted the GSP auction mechanism from Internet advertising to incentivize rational nodes to cooperate, assuming that there are no Byzantine nodes in the network. Usually a mechanism requires payment from the traffic sender which exceeds the total cost in current relay nodes, such that they have incentive to participate. The difference between the payment and total cost is referred to as overpayment. On the other hand, it is natural that the sender wants to be serviced at low cost and hence small overpayment. It has also been proved that the GSP mechanism guarantees lower overpayment than the popular VCG mechanism. Here proposed the FORBID mechanism based on a decentralized reputation system to detect and isolate Byzantine behaviour, assuming that there are no rational nodes or they have been incentivized to cooperate by other schemes. Here separately shown the effectiveness of the two schemes to their target category of misbehaviour, with the assumption the other category of misbehaviour does not exist.

In this research work, make one step further towards appropriate treatment for both categories of misbehaviour in a unified framework. The main contributions are:

3. GSP, FORBID detects malicious behavior in the forwarding stage, and in turn, triggers GSP to update the least cost paths to exclude the Byzantine nodes from future involvement.
4. Rigorously prove in two steps that the proposed routing protocol is cooperation-optimal.
5. Complement the theoretical analysis with extensive experimental evaluations and demonstrate how rational and Byzantine behaviors are distinctly and effectively handled by the unified protocol.

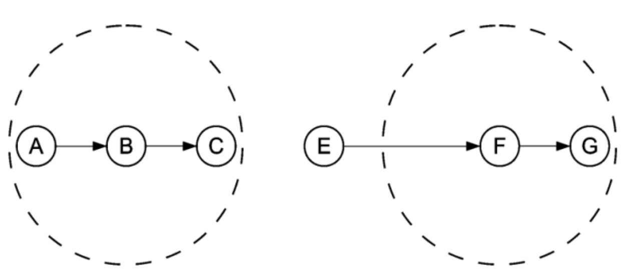


Fig.1.1.Unreliable overhearing. Dashed circle represent the transmission range of centering nodes.

In proposed routing protocol spread the traffic over the nodes lying on different possible paths between the source and the sink, in proportion to their residual energy and received signal strength. The rationale behind traffic spreading is that for a given total energy consumption in the network, at each moment, every node should have spent the same amount of energy. The objective is to assign more loads to under-utilized paths and less load to over-committed paths so that uniform resource utilization of all available paths can be ensured.

Multipath routing is cost effective for heavy load scenario, while a single path routing scheme with a lower complexity may otherwise be more desirable. Comparing the proposed scheme with the directed diffusion and flooding protocols Simulation results show that energy efficient adaptive multipath routing outperforms the traditional routing approaches in terms of network lifetime, load balancing and packet delivery ratio.

1. Eliminate the fundamental assumption on the existence of either kind of misbehavior in previous work.
2. Present a hybrid design that seamlessly incorporates GSP and FORBID in a unified framework. With the possible inclusion of Byzantine nodes in the least cost paths selected by

Terminology

Wireless mesh networks

Wireless Mesh Networks combine static mesh routers (mesh routers and gateways) operating in ad hoc mode with mobile wireless nodes (mesh clients). These networks are, for instance, appropriate to expand network connectivity in regions where access to an infra-structured network is limited. Gateways and mesh routers communicate with the external network (e.g. the Internet) by forwarding each other's traffic (including clients traffic) towards the gateway nodes, which are directly connected to the wired infrastructure. They form the backbone of the network, where mobility is reduced. Mesh clients can be cell phones, laptops or other wireless devices.

Multipath Routing

The multi-path routing models the sensor network into levels according to the hop distance from the sink node to a source node. A node is in level L, if it is L hops apart from the sink. The sink is a level 0 node. All nodes that can talk directly with at least one level N node but cannot talk directly with any level N-1 nodes are defined as level N+ 1 node. Thus, level N nodes have path length of N hops back to the sink. The multipath routing algorithm is composed of two phases: Multipath Construction Phase and Data Transmission Phase by using two messages namely route request message and route reply message.

Route Request message is transmitted when a node enters in the network to execute the neighbour discovery process during the network start-up and also to establish a route to the destination and Route Reply message is initiated when the given source node is reached and to create a new entry in the local neighbour table.

Energy Aware Multipath Routing

In Wireless Sensor Networks the proposed protocol named Energy Aware Multipath Routing in Wireless Sensor Networks is based on the multipath scheme where multiple route exist between each source and the sink. In the following section discuss about system model and assumptions for the proposed protocol and working principle of the proposed protocol.

Dynamic Source Routing Protocol

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Determining source routes requires accumulating the address of each device between the source and destination during route discovery.

Gaussian Random Key

Gaussian process is a statistical distribution where observations occur in a continuous domain, e.g. time or space. In a Gaussian process, every point in some continuous input space is associated with a normally distributed random variable. Moreover, every finite collection of those random variables has a multivariate normal distribution

II. RELATED WORK

Karanbir Singh and Dr. Maninder Singh propose the Wireless Sensor Network focuses on environment interaction and is embedded in the environment itself. Wireless Sensor nodes are called Motes. The main functions of node are: sensing, actuation, processing and communicating information wireless. These networks use radio signals for communication. Jamming is defined as the transmittal of radio frequencies that further interfere with the radio signals used by the inherent sensor networks. it is of two types constant jamming(no message can be sent or received i.e. the complete network is jammed) and intermittent jamming (messages are exchanged between nodes periodically but not consistently) . The solution to this attack is blacklisting of the adversary node [1].

Koushik Banerjee et al propose the Authentication can deliver trustworthiness of the message by recognizing its birthplace. Attackers in a sensor network can alter the contents of a packet as well as inject superfluous bogus packets in the network. The destination node must be able to identify the sender of a packet among original and attacker. Data authentication is a practice of ascertaining the identity of senders. Usually a message authentication code (MAC) is calculated to achieve authenticity [2].

Amr M. Kishk et al, defined WSN is mostly used for gathering application specific information from the surrounding environment. The primary weakness shared by all wireless application and technologies is the vulnerability to security threats. A denial-of-service (DoS) attack is typically one of these threats used by illegitimate users to reduce the functionality and the overall performance of the network. DoS from jamming is difficult to remove it from the reconstructed signal at the receiver with the limit resources available to WSN nodes. Jamming can occur either unintentionally in the form of interference, noise, or collision to disrupt or prevent the signal transmission in WSN. And also, jamming can exhaust the battery energy of the nodes due to multiple retransmission processes. The disturber has many forms and it can be summarized into four types: constant disturber, deceptive disturber, random disturber, and reactive disturber [3].

Mani Amoozadeh et al. argue that jamming attacks can cause collisions in a vehicle platoon, leading to serious multicar pile-up. To present a security model based on Trusted Platform Module (TPM), and describe an application of cooperative driving and its associated threat model. These prior works only discuss a limited number of attacks and none of them consider the actual vehicle longitudinal control in CACC. As a result, these studies ignore other impacts that a security attack might have on a platoon such as string instability. Moreover, none of these studies have carried out any quantitative analysis of the impact of the attacks [4].

Seung Kim et al. define a warehouse model, which consists of the storage containing items equipped with RFID tags and the physical boundary fence. To prevent eavesdroppers outside the fence, multiple jammers are installed in the space between the storage and the fence, and they propose algorithms to optimize the power and the number of jammers. Prior to this jamming optimization study, there have been efforts to protect RFID privacy and fine control the access to RFID. In friendly jamming, showing the theoretical feasibility of using jamming for ensuring confidentiality of wireless communications. Similar studies are also presented for wireless secrecy with various configurations. These are similar to ours in using jamming to achieve wireless secrecy, but in contrast we show how the defensive jamming technique can supplement the existing Wi-Fi security protocol, provide the jammer arrangement algorithms, and discuss practical consideration for real deployment. In friendly jamming this only jams the adversary communication, but ensures the ally communication. It requires a preshared key to generate a jamming signal known to ally, while our mechanism does not depend on any pre-shared secret [5].

Thomas .E et al In this paper, we consider the design of distributed mechanisms in which the outcome is computed by the agents themselves. We propose Distributed MinWork (DMW), a mechanism for solving the problem of scheduling on unrelated machines. We show that DMW is a faithful implementation of the MinWork mechanism, which was proposed by Nisan and Ronen in their seminal work.

We show that in addition to being faithful, DMW protects the anonymity of the losing agents and the privacy of their bids. Furthermore, we show that DMW is efficient as it has polynomial communication and computation costs. We proposed DMW, a distributed mechanism for job scheduling on unrelated machines. The agents execute a distributed Vickrey auction for each of the tasks to determine the allocation and the payment. We showed that our proposed mechanism is a faithful implementation of the truthful MinWork and thus, agents will adhere to the distributed protocol in order to maximize their utility. Furthermore, we showed that the mechanism preserves the privacy of the losing agents by not revealing their identities or their bids. Lastly, we showed that it is polynomial in terms of communication and complexity costs [6].

III. PROBLEM DESCRIPTION

In the literature, two major approaches are developed for handling routing misbehaviour, either incentivizing nodes to cooperate or punishing nodes that refuse to collaborate. Both approaches essentially treat selfish and malicious behaviours non-discriminatingly. The disadvantages of existing system are Protocol design becomes quite challenging with the involvement of both rational and Byzantine behaviour in the same network.

In this work, we make one step further towards appropriate treatment for both categories of misbehaviour in a unified framework.

The main contributions are:

1. This system eliminates the fundamental assumption on the existence of either kind of misbehavior in previous work.
2. This proposed work present a hybrid design that seamlessly incorporates GSP and FORBID in a unified framework. With the possible inclusion of Byzantine nodes in the least cost paths selected by GSP, FORBID detects malicious behavior in the forwarding stage, and in turn, triggers GSP to update the least cost paths to exclude the Byzantine nodes from future involvement
3. This work rigorously proves in two steps that the proposed routing protocol is cooperation-optimal.

The main Advantages of proposed system are sending packets via multiple paths provide benefits such as route resilience, interference avoidance, and load/energy balancing. The proposed routing protocol is cooperation-optimal.

IV. SYSTEM ANALYSIS

Existing System

To distribute the total traffic among available paths the source node performs traffic allocation based on empirical jamming statistics at individual network nodes. If any path to be disturbed/jammed a routing path is requested an existing routing path is not be updated, the responding nodes along the path will disconnect the routing path.

Disadvantage

- Disturb Wireless Communications
- Proactive / Reactive
  - Constant, random, repeat, deceive
  - Single bit/packet
- Outsider / Insider
- Time Delay

Proposed System

Propose techniques for the network nodes to estimate and characterize the impact of jamming and for a source node to incorporate these estimates into its traffic allocation. This work show that in multi-source networks, this centralized optimization problem can be solved using a multi path routing algorithm based on decomposition in network utility maximization. System formulate this traffic allocation as a lossy network flow optimization problem using portfolio selection theory from financial statistics which allow individual network nodes to locally characterize the jamming impact and aggregate this information for the source nodes. Using Multipath routing mechanism each and every packets transfer to the different network topology. The Energy efficient algorithm is used to manipulate efficient transmission rate and time of the proposed work.

Advantage

The main Advantages of proposed system are sending packets via multiple paths provide benefits such as

- Route resilience,
- Interference avoidance, and
- Load/energy balancing.
- Routing protocol is cooperation-optimal.
- Each time a new routing path is requested or an existing routing path is updated.

V. MODULES

Allocation of traffic across multiple routing paths:

Formulate the problem of allocating traffic across multiple routing paths in the presence of jamming as a lossy network flow optimization problem. Map the optimization problem to that of asset allocation using portfolio selection theory which allows individual network nodes to locally characterize the jamming impact and aggregate this information for the source nodes.

Characterizing the Impact Of Jamming:

In these Module the network nodes to estimate and characterize the impact of jamming and for a source node to incorporate these estimates into its traffic allocation. 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 must be estimated. However, to capture the jammer mobility and the dynamic effects of the jamming attack, the local estimates need to be continually updated.

Effect of Jammer Mobility on Network:

The capacity indicating the link maximum number of packets per second (pkt/s) eg:200 pkts/s which can be transported over the wireless link. Whenever the source is generating data at a rate of 300 pkts/s to be transmitted at the time jamming to be occurring. Then the throughput rate to be less. If the source node becomes aware of this effect the allocation of traffic can be changed to 150 pkts/s on each of paths thus recovers the jamming path.

Estimating End-to-End Packet Success Rates:

The packet success rate estimates for the links in a routing path, the source needs to estimate the effective end-to-end packet success rate to determine the optimal traffic allocation. Assuming the total time required to transport packets from each source s to the corresponding destination is negligible compared to the update relay period.

Optimal Jamming-Aware Traffic Allocation:

An optimization framework for jamming-aware traffic allocation to multiple routing paths for each source node. 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.

VI. SIMULATION AND RESULTS

Simulation Parameters

Simulator	Values
Simulation Area	100 m * 100 m
Number of Nodes	20,30,40,50
MAC Protocol	TMAC
Initial battery capacity	18720joule
Simulation Duration	600 seconds
Output Power	-3dBm
Number of runs	5

Table 1. Simulation Parameters

The Energy Aware Multipath Routing Protocol is implemented in NS2.C# with NS2 is a simulator for Wireless Sensor Networks (WSN), Body Area Networks (BAN) and generally networks of low-power embedded devices. It is based on the OMNeT++ platform. We also implemented an interference-aware routing protocol (MR2) and Low Interference Aware Multipath Routing Protocol (LIEMRO) and we have considered the following simulation parameters as mentioned in Table 9.1 for all the algorithms.

Performance Metrics

Node Energy Consumption (Ea): The node energy consumption measures the average energy dissipated by the node in order to transmit a data packet from the source to the sink. The same metric is used in to determine the energy efficiency level of WSNs. It is calculated as follows:

where M is the number of nodes, $e_{i,init}$ and $e_{i,res}$ are respectively the initial and residual energy levels of node i, S is the number of sink nodes and $data_{Nj}$ is the number of data packets received by sink j.

Data Delivery Ratio (R): This metric represents the ratio between the number of data packets that are sent by the source and the number of data packets that are received by the sink.

This metric indicates both the loss ratio of the routing protocol and the effort required to receive data. In the ideal scenario the ratio should be equal to 1. If the ratio falls significantly below the ideal ratio, then it could be an indication of some faults in the protocol design.

However, if the ratio is higher than the ideal ratio, then it is an indication that the sink receives a data packet more than once. It is not desirable because reception of duplicate packets consumes the network's valuable resources. The relative number of duplicates received by the sink is also important because based on that number

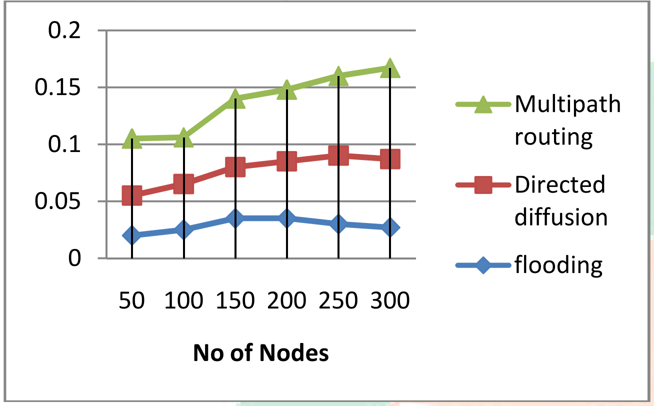
Average Delay: It is defined as the average time between the moment a data packet is sent by a data source and the moment the sink receives the data packet. This metric defines the freshness of data packets.

Simulation results

Under energy constraints, it is vital for sensor nodes to minimize energy consumption in radio communication.

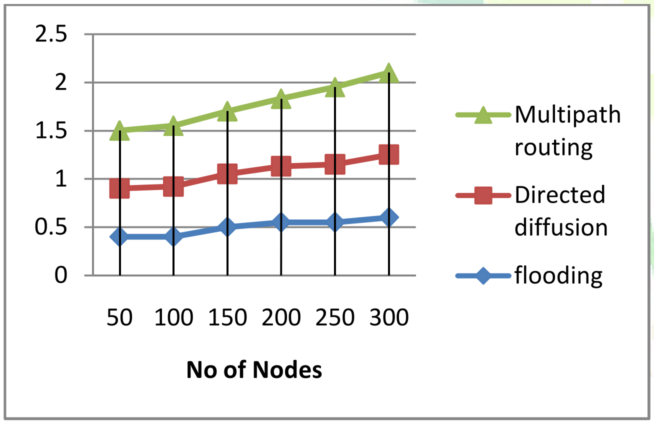
From the results shown in Fig 5, It is observed that there is a lower node energy consumption of our adaptive multipath routing over the other schemes. The flooding is the most costly protocol because the number of hops tends to increase as the node density increases. The directed diffusion obtains further improvement. Figure 5 shows a linear energy increase as the network becomes denser, as more sensor nodes get involved with for both directed diffusion and multipath algorithm.

The reason that the energy consumption of directed diffusion algorithm increases faster than multipath routing algorithm is because the number of sensors participating in the route discovery is less. The improvement of multipath routing is ranging from 10% to 30% when compared with directed diffusion. Such experimental results demonstrate that the energy efficiency of multipath routing is stable and has little impact by the increase of the network size, while the performance of other schemes degrades with larger network size.



Graph 1.a Average Node Energy Consumption

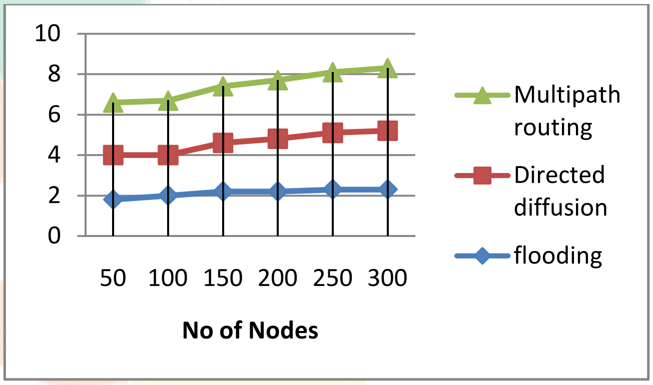
Figure shows the delivery ratio of all the three routing protocols. To eliminate packet loss we use a rate of 5 packets / second. It is found that the delivery ratio of all the protocols increase as the node density increases. When node density is high, there are more nodes available for data forwarding, and this increases the delivery ratio. Flooding offers less packet delivery rates, followed by flooding is directed diffusion; it did not adapt well its behaviour to network size increase. The energy efficient multipath routing protocol has maintained constant delivery rates throughout the simulated scenarios because the paths are selected based on the energy availability.



Graph 1.b delivery ratio

This is a result of the impact of the process it uses to create a routing path. Under energy constraints, it is vital for sensor nodes to minimize energy consumption in radio communication to extend the lifetime of sensor networks. From the results shown in Figure 6, we infer that energy efficient multipath routing tends to reduce the number of hops in the route, thus reducing the energy consumed for transmission.

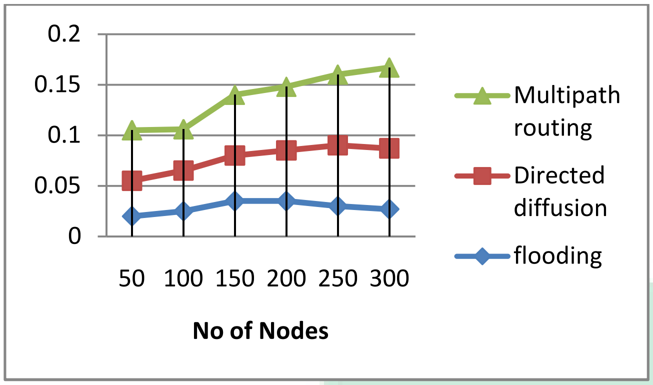
Figure 7 demonstrates the load balancing capability of three routing schemes. Average forwarded data is measured as the average number of data events relayed by a data forwarder for every distinct event delivered to sinks



Graph 1.c load balancing capability

This metric reflects the long-term energy efficiency and potential network fault tolerance. As shown in Figure 7, load balancing capacity of multipath routing increases twice than other routing protocols in most of the density scenarios.

We also study the end-to-end delay performance of these routing protocols. Both route availability delay and propagation delay of data packets contribute to the data latency. The average packet delays under the three schemes are plotted in Figure 8. Additional delay is no more than approximately 1.3 seconds for the 250m transmission ranges. This additional delay grows slowly with the increase of node population. Overall, these results show energy efficient multipath routing protocol’s ability to sustain application performance even for large node densities. Many other attempts at energy savings showed that packet delivery performance usually decreases as a result of increased energy savings. Our results show that energy efficient algorithm can decrease the energy expense of communication with minimum tradeoffs in quality of service. For all traffic conditions multipath routing exhibits less than two-third the data latency of flooding, this is due to the fact that the route selection is more optimized by choosing shortest multi paths against the longer paths.



Graph 1.d Average Data Packet Delivery Delay

VII. APPLICATION

Mobile telephones

One of the best-known examples of wireless technology is the mobile phone, also known as a cellular phone, with more than 4.6 billion mobile cellular subscriptions worldwide as of the end of 2010. These wireless phones use radio waves to enable their users to make phone calls from many locations worldwide. They can be used within range of the mobile telephone site used to house the equipment required to transmit and receive the radio signals from these instruments

Wireless data communications

Wireless data communications are an essential component of mobile computing. The various available technologies differ in local availability, coverage range and performance, and in some circumstances, users must be able to employ multiple connection types and switch between them. To simplify the experience for the user, software can be used, or a mobile VPN deployed to handle the multiple connections as a secure, single virtual network. Supporting technologies include:

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet. Wi-Fi approaches speeds of some types of wired Ethernet. Wi-Fi has become the de facto standard for access in private homes, within offices, and at public hotspots. Some businesses charge customers a monthly fee for service, while others have begun offering it for free in an effort to increase the sales of their goods.

Cellular data service offers coverage within a range of 10-15 miles from the nearest cell site. Speeds have increased as technologies have evolved, from earlier technologies such as GSM, CDMA and GPRS, to 3G networks such as W-CDMA, EDGE or CDMA2000.

Mobile Satellite Communications may be used where other wireless connections are unavailable, such as in largely rural areas or remote locations. Satellite communications are especially important for transportation, aviation, maritime and military use.

Wireless Sensor Networks are responsible for sensing noise, interference, and activity in data collection networks. This allows us to detect relevant quantities, monitor and collect data, formulate meaningful user displays, and to perform decision-making functions

Wireless energy transfer

Wireless energy transfer is a process whereby electrical energy is transmitted from a power source to an electrical load that does not have a built-in power source, without the use of interconnecting wires. There are two different fundamental methods for wireless energy transfer. They can be transferred using either far-field methods that involve beam power/lasers, radio or microwave transmissions or near-field using induction. Both methods utilize electromagnetism and magnetic fields.

Wireless Medical Technologies

New technologies such as mobile body area networks (MBAN) the capability to monitor blood pressure, heart rate, and oxygen level and body temperature, all with wireless technologies. The MBAN works by sending low powered wireless signals to receivers that feed into nursing stations or monitoring sites. This technology helps with the intentional and unintentional risk of infection or disconnection that arises from wired connections.

Computer interface devices

Answering the call of customers frustrated with cord clutter, many manufacturers of computer peripherals turned to wireless technology to satisfy their consumer base Originally these units used bulky, highly limited transceivers to mediate between a computer and a keyboard and mouse; however, more recent generations have used small, high-quality devices, some even incorporating Bluetooth. These systems have become so ubiquitous that some users have begun complaining about a lack of wired peripherals. Wireless devices tend to have a slightly slower response time than their wired counterparts; however, the gap is decreasing.

Computer interface devices such as a keyboard or mouse are powered by a battery and send signals to a receiver through a USB port by way of a radio frequency (RF) receiver. The RF design makes it possible for signals to be transmitted wirelessly and expands the range of effective use, usually up to 10 feet. Distance, physical obstacles, competing signals, and even human bodies can all degrade the signal quality.

Concerns about the security of wireless keyboards arose at the end of 2007, when it was revealed that Microsoft's implementation of encryption in some of its 27 MHz models was highly insecure.

For Estate Agents

Estate agents can work either at home or out in the field. With mobile computers they can be more productive. They can obtain current real estate information by accessing multiple listing services, which they can do from home, office or car when out with clients. They can provide clients with immediate feedback regarding specific homes or neighbourhoods, and with faster loan approvals, since applications can be submitted on the spot. Therefore, mobile computers allow them to devote more time to clients.

Emergency Services

Ability to receive information on the move is vital where the emergency services are involved. Information regarding the address, type and other details of an incident can be dispatched quickly, via a CDPD system using mobile computers, to one or several appropriate mobile units which are in the vicinity of the incident. Here the reliability and security implemented in the CDPD system would be of great advantage.

In courts

Defence counsels can take mobile computers in court. When the opposing counsel references a case which they are not familiar, they can use the computer to get direct, real-time access to on-line legal database services, where they can gather information on the case and related precedents. Therefore mobile computers allow immediate access to a wealth of information, making people better informed and prepared.

In companies

Managers can use mobile computers in, say, and critical presentations to major customers. They can access the latest market share information. At a small recess, they can revise the presentation to take advantage of this information. They can communicate with the office about possible new offers and call meetings for discussing responds to the new proposals. Therefore, mobile computers can leverage competitive advantages.

Stock Information Collation/Control

In environments where access to stock is very limited ie: factory warehouses. The use of small portable electronic databases accessed via a mobile computer would be ideal. Data collated could be directly written to a central database, via a CDPD network, which holds all stock information hence the need for transfer of data to the central computer at a later date is not necessary. This ensures that from the time that a stock count is completed, there is no inconsistency between the data input on the portable computers and the central database.

Credit Card Verification

At Point of Sale (POS) terminals in shops and supermarkets, when customers use credit cards for transactions, the intercommunication required between the bank central computer and the POS terminal, in order to effect verification of the card usage, can take place quickly and securely over cellular channels using a mobile computer unit. This can speed up the transaction process and relieve congestion at the POS terminals.

Taxi/Truck Dispatch

Using the idea of a centrally controlled dispatcher with several mobile units (taxis), mobile computing allows the taxis to be given full details of the dispatched job as well as allowing the taxis to communicate information about their whereabouts back to the central dispatch office. This system is also extremely useful in secure deliveries ie: Securicor. This allows a central computer to be able to track and receive status information from all of its mobile secure delivery vans. Again, the security and reliability properties of the CDPD system shine through.

VIII. CONCLUSIION AND FUTURE WORK

Conclusion

Energy resource limitations are of priority concern in sensor networks. Distributing the load to the nodes significantly impacts the system lifetime. The adaptive multipath routing protocol is capable to search multiple paths and aims to allocate the traffic rate to each path optimally. Simulation results show that our proposed scheme has higher node energy efficiency, than the directed diffusion, and flooding. The limitation in our scheme is the RSSI values which are used, are not constant throughout the simulation period, moreover the fading and interference caused by wireless environments are not taken into consideration this poses a limitation on identifying the network performance in real world scenario. There are several future works we would like to focus on. First, how to guarantee the delivery of packets under situations where non-uniform transmission ranges exist. Second to improve the algorithm to include the integration of data aggregation and finally the support of node with limited mobility. An optimal solution to this problem especially for mobile sensor networks is still an open question.

There are two types of nodes which are used here one is primary and the other is alternate. At the end of the route formation one primary path and multiple alternate paths are built and all nodes except the primary paths nodes are put to sleep mode which helps us to save energy and generate a collision free environment, the primary path is used to transmit the data from source to the sink and if the route disrupts, the next best alternate route is used for the purpose and if no path exists between the source and destination then the route discovery algorithm calls. The simulation result finds the latency, packet delivery ratio, average control packet over head and total energy consumed.

Future Work

One of the weaknesses of the current model is the restriction to homogeneous system assumption in which all servers are identical and all arrival streams have similar characteristics. This assumption is far from reality in all applications of interest. The optimal splitting rule, in the absence of queue backlog information, in such practice will potentially depend on the load as well as the degree of asymmetry among servers and arrival statistics. Following insights from the result of this work, we conjecture that it is optimal (in an average delay sense) for each job to be distributed in such a way that the random vector associated with various pieces across secondary queues is minimized (in some multivariate stochastic sense). That is, in an asymmetric setting, the result obtained above can be extended to identify the policy which minimizes the average delay.

IX. REFERENCES

[1] THE CLONE ATTACK IN SENSOR NETWORK – ANALYSIS AND DEFENSE by Karanbir Singh and Dr. Maninder Singh published in International Journal in Applied Studies and Production Management Volume1, Issue 3, 15 May- 15 August 2015

[2] Hybrid Radio Frequency/Free-Space Optics (RF/FSO) Wireless Sensor Network: Security Concerns and Protective Measures. By Koushik Banerjee, Hemant Sharma and Anasuya Sengupta Proceedings of the First International Conference, IEM OPTRONIX 2014

[3] Proposed Jamming Removal Technique for Wireless Sensor Network by Amr M. Kishk, Nagy W. Messiha , Nawal A. El-Fishawy , Abdelrahman A. Alkafs and Ahmed H. Madian International Journal of Scientific Research in Network Security and Communication Volume-3, Issue-2 30 Apr 2015.

[4] Security Vulnerabilities of Connected Vehicles Streams and their Impact on Cooperative Driving by Mani Amoozadeh , Arun Raghuramu , Chen-Nee Chuah , Dipak Ghosal H. Michael Zhang , Jeff Rowe , Karl Levitt.

[5] A jamming approach to enhance enterprise Wi-Fi secrecy through spatial access control by Yu Seung Kim, Patrick Tague, Heejo Lee, Hyogon Kim Springer Science+Business Media New York 2015

[6] Akyildiz, I., Su, W., Sankarasubramaniam, Y. e Cayirci, E. "A Survey on Sensor Networks", IEEE Communications Magazine, pp. 102-114, 2002

[7] S. Tilak, N. B. Abu-Ghazaleh and W. Heinzelman, "A Taxonomy of Wireless Micro-Sensor Network Models", Mobile Computing and Communications Review, Vol. 6, No. 2, pp. 28-36, 2002.

[8] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing," in Proc. of ACM/IEEE MobiCom'01, Rome, Italy, July 2001, pp. 70 – 84.

[9] R. Shah and J. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in Proc. of IEEE WCNC'02, Orlando, FL, March 2002, pp. 350–355.

[10] K. Wu and J. Harms, "On-demand multipath routing for ad hoc networks," in Proc. of European Personal and Mobile CommunicationsConference (EPMCC), Vienna, Austria, Feb. 2001.

[11] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," in Proc. of ACM MobiHoc'01, Long Beach, CA, USA, Oct. 2001.

[12] J. Chang and L. Tassiulas, "Energy conserving routing in wireless adhoc networks," in Proc. of IEEE INFOCOM'00, Tel-Aviv, Israel, March 2000, pp. 22–31.

[13] Q. Li and J. Aslam and D. Rus, "Hierarchical Power-aware Routing in Sensor Networks", In Proceedings of the DIMACS Workshop on Pervasive Networking, May, 2001.

[14] S. Dulman, T. Nieberg, J. Wu, P. Havinga, "Trade-off between Traffi Overhead and Reliability in Multipath Routing for Wireless Sensor Networks", WCNC Workshop, New Orleans, Louisiana, USA, March 2003.

[15] Jian Wu, Stefan Dulman, and Paul Havinga " Reliable Splitted Multipath Routing for Wireless Sensor Networks" Proceedings of Building intelligent Sensor Networks (BISON 04), China 2004.