Reliable and Secured Routing in Wireless Networks

Vikas Verma
Assistant Professor,
Department of Computer Applications,
CGC, Landran

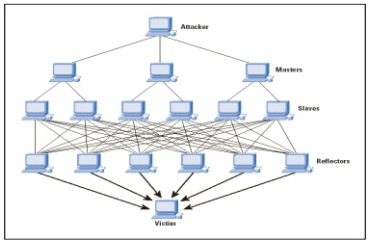
Abstract
The rapid need of wireless demands a great deal of security and reliable routing in order to keep all the data sources and equipments secure. In order to develop efficient and robust protocols, it is essential to understand the inherent characteristics of wireless networks such as connectivity, coverage and varying channel conditions. Factors such as multipath fading, shadowing and path loss cause wireless channel variability at different timescales (in the milliseconds, seconds and tens of seconds timescale respectively). Node mobility also plays an important role in determining wireless channel variability. Changes in network connectivity and topology caused by node mobility and fluctuating channel conditions mean that protocols have to make design decisions based on partial or outdated network state information. These variations, however, present opportunities to leverage the dynamic (varying) nature of these networks to improve application-level performance. In this paper we proposed efficient routing and scheduling algorithms that adapt to changing network conditions caused by varying link quality or node mobility to improve user-level performance.

Keywords: Scheduling Algorithm, Routing, Wireless, Pushback Model

Introduction

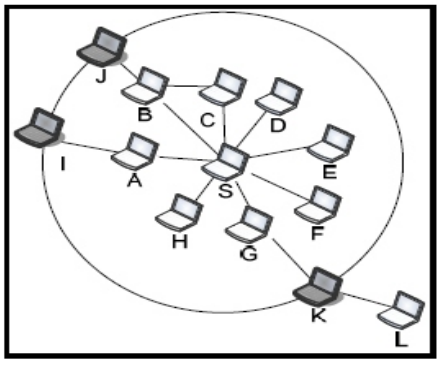
In the latest research on Wireless Networks, researchers are trying to find and overcome the limitations of wireless networks such as limited energy resources, ranging energy consumption by location, the high cost of transmission, and limited processing capabilities. All these features of wireless are not present at all in cable networks, where energy consumption is not at all a problem, the cost of transmission of the data is very cheap and nodes have lot of processing power. We need to find the new ways for this new generation to work on the networks. So in order to succeed we have to enhance the routing criteria. Routing is the process used by the data communication networks to deliver packets from a source device to a destination device. In WSN, the three main routing categories are:

- Flat-based routing: In this, all nodes have an equal role and perform equal tasks.
- Location-based routing: In this, all nodes have their roles to route data according to their locations.
- Hierarchical routing based: In this, all nodes have their own different roles of others.



How to Route in Wireless Networks

The broadcast nature of wireless networks allows a much richer set of approaches to be taken when forwarding packets between source and destination than traditional hop-by-hop forwarding along pre-specified paths. These strategies fall into two broad categories - opportunistic forwarding, which exploits relay diversity by opportunistically selecting an overhearing relay as a forwarder, and cooperative forwarding, which relies on the synchronized transmissions of relays to reinforce received signal strengths. Our objective is to understand which among these two approaches provides higher performance (throughput) in presence of multiple competing and interfering network flows.



Routing zone with radius r=2

We observe that opportunism outperforms cooperation and identify interference resulting from the larger number of transmissions under cooperative forwarding as a cause for mitigating the potential gains achievable with cooperative forwarding .Mobility in wireless networks introduces additional sources of channel variation and makes routing even more challenging. Frequent changes in network topology require additional control overhead for gathering link state information needed for determining routes.

Related Work

According to routing includes origin packets in the direction that is referred as a destination by giving packet delivery relation. This thing guarantees the efficient delivery of packets from source to destination.

By implementing this work the failure issue of the nodes reduced considerably. This rule enhances the life of wireless detector by estimating the interval of nodes. The Proposed protocol selects a cluster head that have a highest energy. The cluster head sends the packets to the gateways. XU Jiu-qiang. projected the prominent rule for connecting nodes. This rule provides a way to attach the nodes of wireless network.

Experimental Design

The proposed model has been designed for the minimal use of energy and hence minimum energy consumption over the wireless networks along with high energy level path selection for the Reliable Routing and Scheduling in Wireless Networks. It starts with development of nodes to execute the essential simulation and then implementation of necessary code for pushback algorithm for detecting the dead nodes. After implementing the energy based path selection for load balancing now implement the best among various paths using Game Theory.

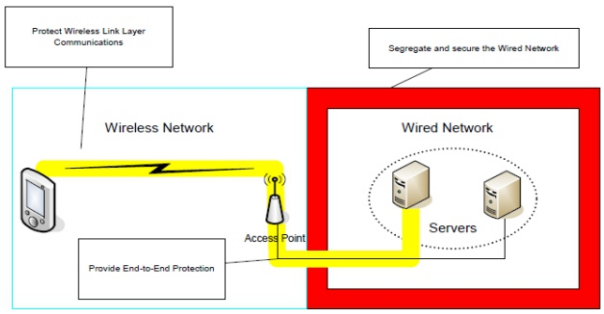
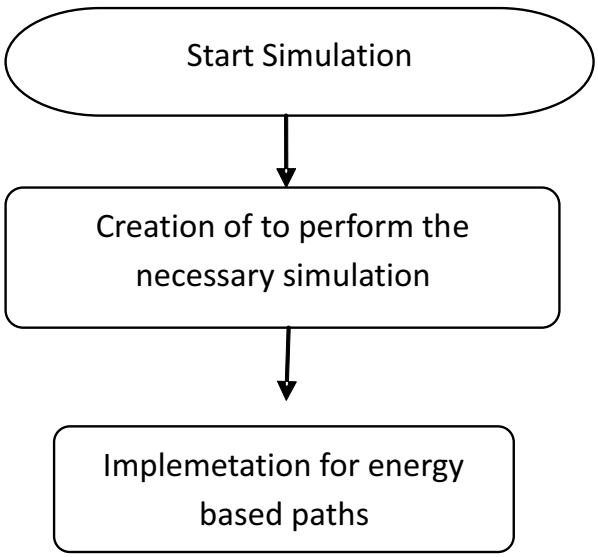
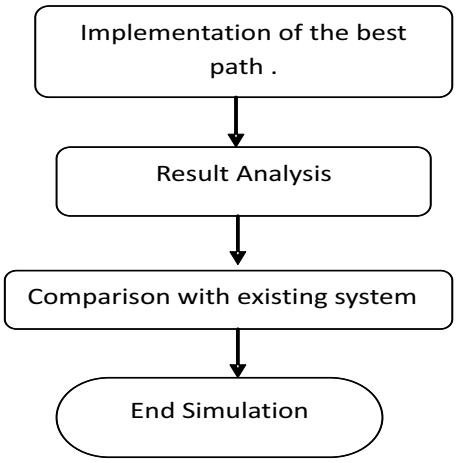


Figure1. Design Strategy

Having an accurate model for the push back process is important for this and identifying all of the intrusions that may occur can lead to more inaccurate and non-realistic decision making After testing a model with a more detailed push back process we found that a lot of the routing process got easier and more secured. It has been enhanced for the dual layer, which checks the network performance evaluation and security level of the target nodes in order to protect nodes from intruders. Here is the flowchart for the experimental design.





Flow chart of work planning
The following algorithm defines the proposed pushback agent model in detail:

Algorithm 1: pushback routing algorithm

1) Choose the node
2) Connect the wireless node during the startup phase.
3) Nodes starts sending the neighbor setup phase.
4) When a wireless node needs to send the data, routing algorithm starts.
5) Routing algorithm calls pushback model.
6) Pushback model analyzes the nodes.
   a) Node replies with initial acknowledgement
   b) If initial acknowledgement is found successful
      i) Check the node availability
      ii) Check the available queue size.
      iii) Give acknowledgement
7) If b (iii) returns true, start the process
      i) Share the information
      ii) Send the query code
      iii) Destination node will reply with the query code.
      iv) Establish the connection
      v) Start routing the process

Result Analysis

The overall results of the simulation has been obtained from various network performance parameters, which are collected in terms of data in the terms of data propagation, queuing delay and other related parameters.

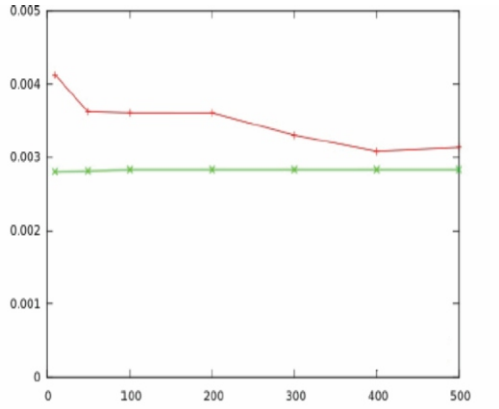


Fig 2. Performance evaluation based upon the transmission delay

Figure 1 gives the performance result of transmission delay obtained from proposed model simulation. The delay tells the performance of the network. The proposed model has been tested with constant bit rate at the rate of 100 kbps over which are targeted from source to destination.

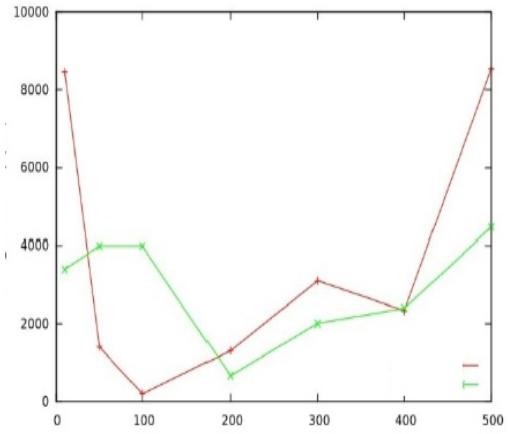


Fig 3. Performance evaluation based upon the energy consumption

Energy consumption in wireless network is evaluated for the overall performance of the proposed model in order to estimate the overall remaining energy on the nodes. All the nodes transmit the data packets in order to send these packets they lose some of the energy which has been tested. The energy less nodes and the more energetic nodes are the most susceptible nodes in the routing process. Those nodes have to be skipped from the routing for secured and efficient routing process.

Conclusion

The proposed model has been considered as the efficient method for Reliable and secured routing in Wireless Networks which is achieved by implementing pushback algorithm which gives security assurance and reliable routing between source and destination. The proposed model has

been tested under various circumstances under different network topology which returns the primary performance parameters. The resource utilization returns the status of the free path with respect to their usage, which is used by load balancing function to elect the best possible path available for data transfer. The proposed model has been found efficient in terms of secured path as the best routing paths has been achieved by other researchers as well but there always a big question mark on the security of the path chosen. Proposed model is implemented in such a way that it has been found efficient in the term s of the evaluated performance from the given wireless network.

References

[1] L. Barrie`re, P. Fraigniaud, L. Narayanan, and J. Opatrny, "Robust Position-Based Routing in Wireless Ad Hoc Networks with Unstable Transmission Ranges," J. Wireless Comm. and Mobile Computing, vol. 2, no. 3, pp. 141-153, 2001.

[2] M. Battelli and S. Basagni, "Localization for Wireless Sensor Networks: Protocols and Perspectives," Proc. IEEE Canadian Conf. Electrical and Computer Eng., (CCECE '07), pp. 1074-1077, Apr. 2007.

[3] M. Zorzi, "A New Contention-Based MAC Protocol for Geographic Forwarding in Ad Hoc and Sensor Networks," Proc. IEEE Int'l Conf. Comm. (ICC '04), vol. 6, pp. 3481-3485, June 2004.

[4] Malekzadeh M, Ghani AAA, Subramaniam S. "A new security model to prevent denial-of-service attacks and violation of availability in wireless networks". International Journal of Communication Systems 2012.

[5] Wu D, Wang R, Zhen Y. "Link stability-aware reliable packet transmitting mechanism in mobile ad hoc network". International Journal of Communication Systems 2012.

[6] Singh G, Kumar N, Verma AK. "Ant colony algorithms in MANET: A review". Journal of Network and Computer Applications 2012; 35(6):1964 – 1972, doi:http://dx.doi.org/10.1016/j.jnca.2012.07.018. URL http://www.sciencedirect.com/science/article/pii/S1084804512001701.

[7] Zhang Z, Feng Z. "Two-stage updating pheromone for invariant ant colony optimization algorithm". Expert Systems with Applications 2012; 39(1):706 – 712, doi:http://dx.doi.org/10.1016/j.eswa.2011.07.062. URL http://www.sciencedirect.com/science/article/pii/S0957417411010244.