International Journal on Applications in Electrical and Electronics Engineering
Volume 1: Issue 7: July 2015, pp 18-21. www.aetsjournal.com ISSN (Online) : 2395-3527

Energy Efficient Reliable Wireless Networking with High Lifetime and Security

S.Arul Murugan, P.Matheswaran, R.Logarasu

Abstract— The sensing capabilities of networked sensors are affected by environmental factors in real deployment and it is imperative to have practical considerations at the design stage in order to anticipate this sensing behaviour. Wepropose a new metric, the drain rate, to forecast the lifetime of nodes according to current traffic conditions. This metric is combinedwith the value of the remaining battery capacity to determine which nodes can be part of an active route.The existent security threats an adhoc network faces,the security services required to be achieved and thecountermeasures for attacks in routing protocols.The authorized nodes keep sending Request-to- Send (RTS) frames to the access point node in order to access to shared medium and start data transfer.We develop energy consumption models that take into account energy consumption due to data packets, control packets and retransmission.

Keywords— STDFF, D Flip Flop, Negative Edge trigger, Conventional Transistor.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is an autonomoussystem it consists of a variety of mobile hosts forming a temporary network without any fixed infrastructures. The problem is enlarge by the fact of that routing usually it needs to really on their trustworthiness all the nodes are participating in their routing process. Since it is mainly difficult to dedicate routers and other infrastructures in such a network, all these nodes are self-organized and collaborated to each other. All their nodes as well as the routers it can move aboutit freely and thus this network topology is highly dynamic. The minimum hop count metrics choose arbitrarily among their different paths of same minimum length, regardless of their often large differences in throughput among those paths and ignoring the possibility the longestpath might offer higher throughput.Transmission power control is used to improve the throughput capacity in a wireless packet network. Such studies motivate the definitionof a link cost that is a function of both the energy required for a singletransmission attempt across the link and the link error rate. Thiscost function captures the cumulative energy expended in reliabledata transfer, for both reliable and unreliable link layers. MDR extends nodal battery life and the duration of paths, while CMDR also minimizes the total transmission energyconsumed per packet. Combined with the value of the remainingbattery capacity, this metric is used to establish whetheror not a node can be part of an active route.

S.Arul Murugan,PG Scholar, Selvam College of Technology, Namakkal.
P.Matheswaran, R.Logarasu , Assistant Professor, Selvam College of Technology, Namakkal. (Email: cavinpalanisamy@gmail.com , kukhapprabu@gmail.com, bkarthi08@gmail.com, ram_trichy12@yahoo.co.in)

II. RELATED WORKS

The probabilistic approach is a deviation from the idealisticassumption of uniform circular disc for sensing coverage usedin the binary detection model. Along this guide path, data packets are greedily progressedtoward the destination through nodes' cooperationwithoututilizing the location information. The proposed flip flop has small area, power and delay overheads and good radiation hardening capabilities. A multiplexer is used to select the correct value as final output according to the fault indication signal.The shortcut tree routing(STR) protocol that provides the near optimal routing path as well as maintains the advantages of the ZigBee tree routingsuch as no route discovery overhead and low memory consumption. TheIndependent basic service set is used in this research that has no backbone infrastructure andconsists of at least two wireless stations. Theoretical analysis shows thatHS can spread a given number of message copies in an optimal way when the inter-meeting time between any two nodes andbetween a node and a community home follows independent and identical exponential distributions, respectively. Datadelivery source routing by multilayer encryptions or end-to-end re-encryptions by a virtual circuit.Regardless of their implementationdetails, these schemes all aim to hide real packet sourcesand destinations in both route discovery and packet forwardingfrom a limited number of local and internal attackers. In thispaper, we show that it is feasible for a passive global adversaryto accurately discover the traffic pattern despite the use of these elegant schemes. One assumes constant rates and the other assumesan arbitrary process. A shortest cost path routing algorithm is proposedwhich uses link costs that reflect both the communicationenergy consumption rates and the residual energy levels at the twoend nodes. To estimate unicast linkquality based on that of broadcast. It is, however, difficult toprecisely estimate unicast link quality via that of broadcast,because temporal correlations of link quality assumecomplex patterns and are hard to model.

III. TRAFFIC ANALYSIS

Traffic analysis is the process of intercepting andcollecting messages on the way to track importantinformation from patterns in communication. Thatinformation is not leaking or not modified just domonitoring and analysis activities. It can get informationfrom the monitor frequency and timing

packets.In evidence-based statistical traffic analysis model, every captured packet is treated as evidence supporting a point-to-point (one-hop) transmission between the sender and the receiver. A sequence of point-to-point traffic matrices is created, and then they are used to derive end- to-end (multihop) relations. This approach provides a practical attacking framework against Mobile Wireless Network but still leaves substantial information about the communication patterns undiscovered. Statistical traffic analysis attacks have attracted broad interests due to their passive nature, i.e., attackers only need to collect information and perform analysis quietly without changing the network behaviour. The predecessor attacks and disclosure attacks are two representatives.However, all these previous approaches do not work well to analyse traffic because of the following three natures of Mobile Wireless Network:

A.The broadcasting nature

In wired networks, a point-to-point messagetransmission usually has only one possible receiver. While in wireless networks, a message is broadcasted, which can have multiple possible receivers and so in curs additional uncertainty.

B. The ad hoc nature

Mobile Wireless Network lack network infrastructure and each mobilenode can serve as both a host and a router. Thus, it is difficult to determine the role of a mobile node to be a source, a destination, or just a relay.

C. The mobile nature

Most of existing traffic analysis models does not takeinto consideration the mobility of communication peers, which make the communication relations among mobile nodes more complex.

Sensor Deployment

First we use a heuristic to computethe deployment locations. A heuristic is then used to schedule the sensor nodes such thatthe network lifetime is maximum.

Sensor Deployment Approach

1: Set Input: X , t
2: Output: Optimal location of X and sensor schedule
3: Deploy X randomly
4: Compute upper bound of network lifetime
5: Recompute sensor node such that the upper bound of network lifetime is maximum
6: Design sensor schedule using the proposed heuristic for sensor scheduling such that the network lifetime upper bound is achieved

A heuristic for Sensor Deployment

1: Place sensor nodes randomly
2: **for** i =1 to m **do**
3:**if** Xi does not monitor any target **then**
4: Move Si to the least monitored target
5:Recompute sensor-target coverage matrix
6:**end if**
7: **end for**
8: X = Sensor nodes sorted in ascending order of number of targets it covers
9: **for** i =1 to m **do**
10: **repeat**
11: Place Xi at the center of all targets it covers
12: Move Xi to the center of all targets it covers and its next nearest target
13: **if** Xi can cover a new target **then**
14: Recompute sensor-target matrix
15:**else**
16: Discard move
17:**end if**
18:**until** Xi can cover another target
19: **end for**
20: Compute upper bound of network lifetime

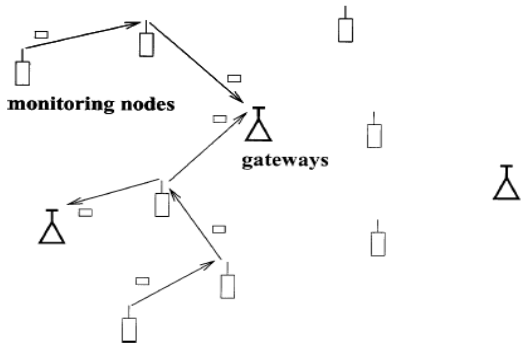

Fig.1 Data Transmission using Gateways

IV. PROTOCOL TECHNIQUES

A.Sleep Protocol

Sleep protocol mainly helps to getting the node energy value has becomes toocompared to threshold value. The sleep protocol having two different typeof modes.

(1)As soon as you notice you are awake, observe the urge and back to sleep immediately.

(2)To move at all, at only once, and it's gently so as not to wake up.

B.Leach Protocol

Leach protocol helps in selecting the weightiest node as the forward node as soon as the sleep protocol makes the previous node to sleep. For selecting the best one, the protocol follows a rapid analysis of nodes on its weighage.

V.PROPOSED METHOD DESIGN

A. Energy Efficiency

To this end, reliabilityand energy cost of routes must be considered in routeselection. The key point is that energy cost of a route isrelated to its reliability. If routes are less reliable, theprobability of packet retransmission increases. Thus, alarger amount of energy will be consumed per packet dueto retransmissions of the packet. When a node transmits the

packets from source to destination, the energy value decreases in step by step process. When a source node has reached the threshold value and the distance is very high then the data packets didn't reach the destination; it takes a long time to reach the destination. So the efficiency has decreases.

B. Path node Selection

When the node energy value becomes low the data loss will be occurred. For to improve the efficiency and reduce the delay the path (intermediate) node has been selected. The source will be transmits the data to destination towards the path node. The path node receives the packets it's transmits the data to long distance.

VI. Experimented Results

The traffic files are generated such that the source and destination pairs are randomly spread over the entire network. The scenariofiles determine the mobility of the nodes.

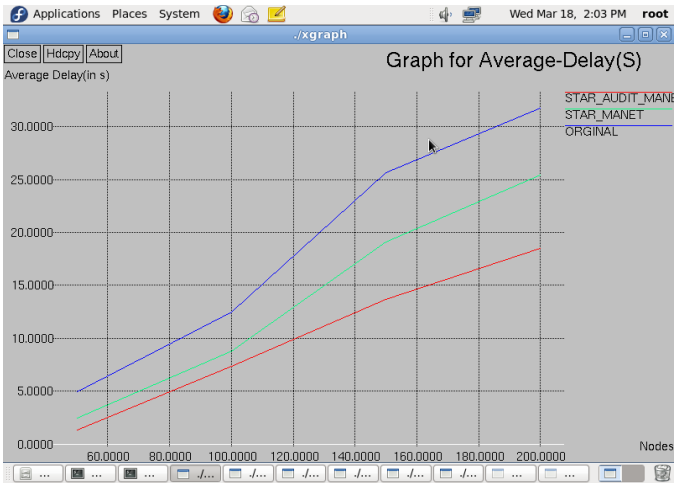

Fig .2Average Delay of Transmission

The above graph symbolizes the average delay of transmission of packets within the total group of nodes. A Typical Transmission and Projected Transmission are compared here. From the simulation results it is clear that the delay is reduced in the proposed approach than that of the prevailing system.

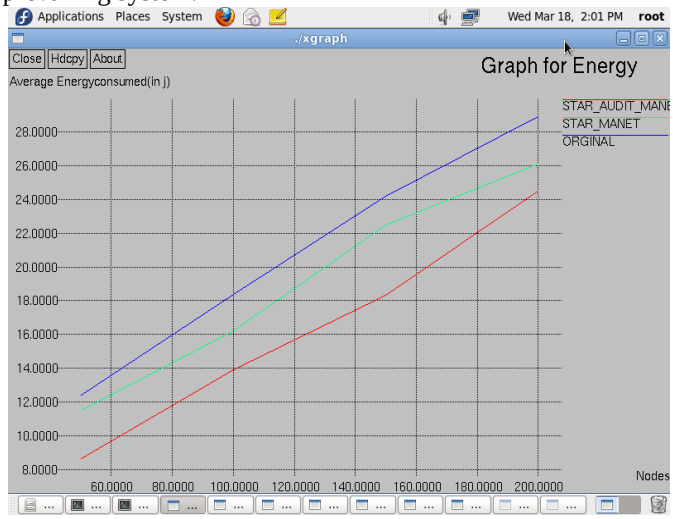

Fig.3 Energy Consumption Graph

The above graph symbolizes the average energy consumed for packet data transmission within the total group of nodes. A Typical Transmission and Projected Transmission are compared here. From the simulation results it is clear that the energy consumption is reduced in the proposed approach than that of the prevailing system.

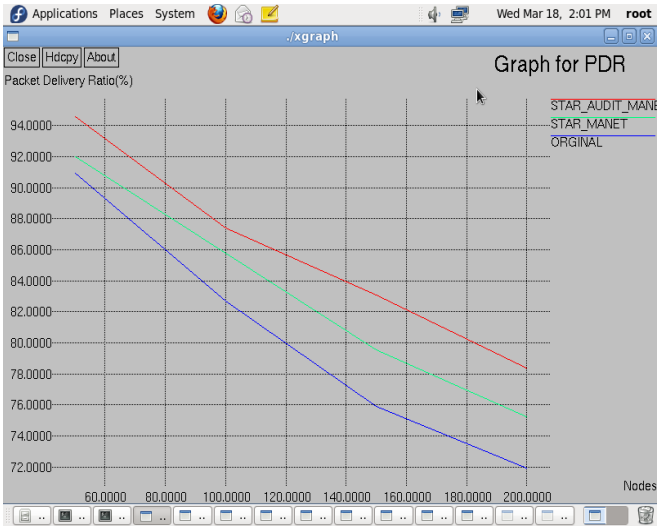

Fig .4 Packet Delivery Ratio in Transmission

The above graph symbolizes the Packet Delivery Ratio in transmission of packets within the total group of nodes. From the simulation results it is evident that the Packet Delivery Ratio is increased in the suggested approach than that of the prevailing systems.

Throughput value denotes that the efficiency has improved as the delay is reduced. The output signal shows the ratio of source value to the received value.From the simulation results (Fig .5) it is evident that the overall throughput is increased in the proposed approach than that of the prevailing systems.

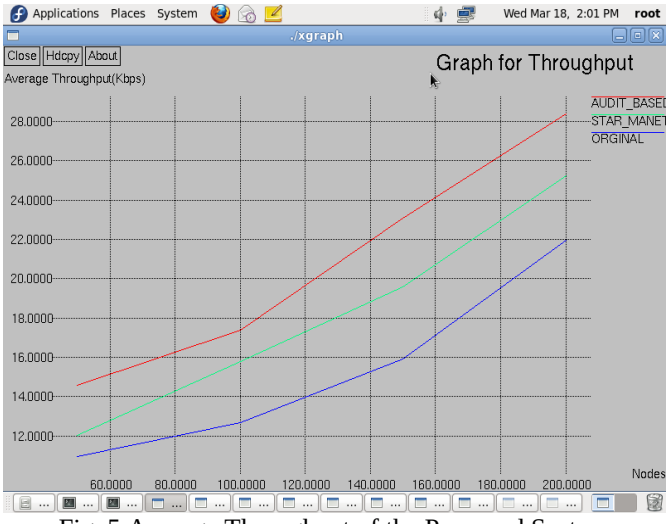

Fig .5 Average Throughput of the Proposed System

VII. CONCLUSION

Conversely, the implementation of suchmechanisms does not only mitigate the jamming attack effects, it also increases the overallperformance above the normal state of the networkconstraints. Even adhoc networks have vast potential, still there are many challenges left to overcome. From the captured packets, Network constructs a sequence of traffic matrices to derive the traffic matrix, and then uses a heuristic data processing model to reveal the hidden traffic patterns from the end-to-endmatrix.

REFERENCES

[1] N. Bartolini, T. Calamoneri, T. La Porta, and S. Silvestri, "Mobile sensor deployment in unknown fields," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–5.

[2] I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing Rrotocol", *IETF Internet Draft*, v.15, November 2008.

[3] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.

[4] T.H. Cormen and C.S. Charles, E. Leiserson, and R.L. Rivets, Introduction to Algorithms, second ed. MIT Press, 2001.

[5] W. Dai, "Two Attacks against a PipeNet-Like Protocol Once Used by the Freedom Service", http://weidai.com/freedomattacks.txt, 2013.

[6] Md. GolamRashed, M. HasnatKabir, ShaikhEnayetUllah, "WEP: An Energy Efficient Protocol for Cluster based Heterogeneous Wireless Sensor Networks", International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.2, March 2011.

[7] S. Gold, "A PspiceMacromodel for Lithium-Ion Batteries," Proc. 12th Ann. Battery Conf. Applications and Advances, pp. 215-222, Jan. 1997.

[8] A. Habib, M. Hefeeda and B. Bhargava. "Detecting Service Violations and DoS Attacks", In The 10th Annual Network and Distributed System Security Symposium 2003. San Diego, California. pp. 177- 189.

[9] D. Huang, "Unlinkability Measure for IEEE 802.11 Based MANETs", IEEE Trans. Wireless Comm., vol. 7, no. 3, pp. 1025- 1034, Mar. 2008.

[10] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour "A Survey of routing attacks in mobile ad hoc networks", *IEEE Wireless Communications*, page 86, 2007.

[11] A. Krause, R. Rajagopal, A. Gupta, and C. Guestrin, "Simultaneous placement and scheduling of sensors," in Proc. Int. Conf. IPSN, 2009, pp. 181–192.

[12] P. Liaskovitis and C. Schurgers, "Energy Consumption of Multi- Hop Wireless Networks under Throughput Constraints and Range Scaling," Mobile Computing and Comm. Rev., vol. 13, no. 3, pp. 1-13, 2009.

[13] Y. Li and S. Gao, "Designing k-coverage schedules in wireless sensor networks," J. Combinat. Opt., vol. 15, no. 2, pp. 127–146, 2008.

[14] Y. Liu, R. Zhang, J. Shi, and Y. Zhang, "Traffic Inference in Anonymous MANETs," Proc. IEEE Seventh Ann. Comm. Soc. Conf. Sensor Mesh and Ad Hoc Comm. and Networks (SECON '10), pp. 1-9, 2010.

[15] NishuGarg and R.P.Mahapatra, "MANET Security Issues", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[16] C. Perkins, E. Royer and S. Das, "Ad Hoc On Demand Distance Vector (AODV) Routing", draft-manet-ietf-aodv-8.txt, *IETF*, Work in Progress, March 2001.

[17] Ping Yi, Yue Wu and FutaiZou and Ning Liu, "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[18] SaiJi, Liping Huang and Jin Wang, "A Distributed and Energy-efficient Clustering Method for Hierarchical Wireless Sensor Networks", International Journal of Future Generation Communication and Networking Vol. 6, No. 2, April, 2013.

[19] J. Vazifehdan, R. Prasad, and I. Niemegeers, "Minimum Battery Cost Reliable Routing in Ad Hoc Wireless Networks," Proc. Eighth IEEE Consumer Comm. and Networking Conf., Jan. 2011.

[20] Q. Wang, M. Hempstead, and W. Yang, "A Realistic Power Consumption Model for Wireless Sensor Network Devices," Proc. Third Ann. IEEE Comm. Soc. Sensor and Ad Hoc Comm. and Networks (SECON '06), pp. 286-295, Sept. 2006.

[21] J. Wexler, "All About Wi-Fi Location Tracking," Network World, http://features.techworld.com/mobile-wireless/2374/all-about- wi-fi-location-tracking/, 2004.

[22] K. Wu, Y. Gao, F. Li, and Y. Xiao, "Lightweight deployment-aware scheduling for wireless sensor networks," Mobile Netw. Appl., vol. 10, pp. 837–852, Dec. 2005.

[23] J. Wu and S. Yang, "Optimal movement-assisted sensor deployment and its extensions in wireless sensor networks," Simul.Model.Pract.Theory, vol. 15, no. 4, pp. 383–399, 2007.