IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Enhanced Energy and Secured Using Position Based Routing Protocol Design for Wireless Mesh Networks

Dr. K. Kumaravel[1], Ms. V. Renugadevi[2]

Head/Asst. Professor (SG), Department of Computer Science, Dr.N.G.P. Arts and Science College, Coimbatore[1]

Research Scholar, Department of Computer Science, Dr.N.G.P. Arts and Science College, Coimbatore[2]

Abstract: The more transmission time and increased failure rate of wireless mesh paths, the issues faced to provide trustworthy message distribution for high secured and power-efficient manner. Past researches without rebroadcast consume lots of energy. In proposed system consist a new multi-path power-control transmission and sleep-wake scheme. It achieving a good balance between overall the energy efficiency and the end-to end packet delay. The proposed system combines power control with multipath routing and packet combining at the destination With carefully designed power control strategies, current research consumes much less energy than the conventional one-path transmission scheme without retransmission. Our results show the proposed protocol is highly energy efficient with low intermediate packet delays, which reduces the power consumed and also focus on disconnected multipath with higher security.

Index Terms: Trustworthy Message, Intermediate Nodes, Power Consumed.

I.INTRODUCTION

WMN is a communications network which made up of radio nodes organized in a mesh topology. WMN is also a form of wireless ad hoc network. Wireless mesh networks often contain of mesh clients, mesh routers and gateways. The mesh clients are provide laptops, cell phones and so on.while the mesh routers forward traffic to and from the gateways which may, but not necessary connect to the Internet.

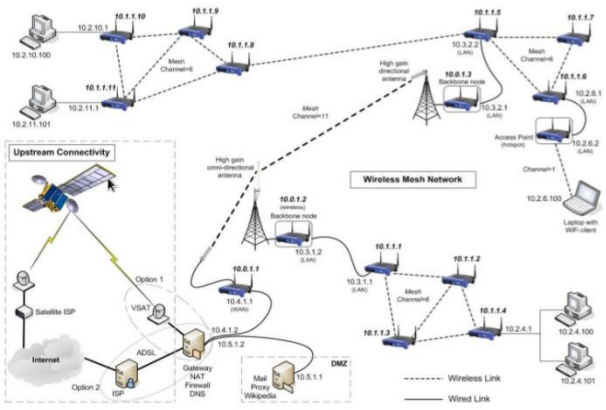


Fig.1: the basic structure of Wireless Mesh Networks

The coverage area of the radio nodes are working as a single network and sometimes it's called a mesh cloud. The Access to this mesh cloud is dependent on the radio nodes are working harmony with each other to create a radio network. Always mesh network is reliable and offers redundancy. When one node can no longer operate, and then the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. Self form and self heal possible in WMN.

Wireless mesh networks implemented with a variety of wireless technology including 802.11, 802.15, 802.16, cellular technologies or combinations of more than one type

II. RELATED WORK

[1] In this paper, they consider the Spectrum Squeeze: The encounter for Band width envisioned a potential fight for wireless bandwidth frequencies between the television networks and telecom service providers. Shaw Communications announced and it would use Wi-Fi as a next-generation wireless network of choice in hope of future customer demand .But another option, still in the research phases, here we have assigned radio frequencies to wireless communications now work very harder. Several organizations and educational institutions are taking the Research & Development path to solving the bandwidth limitation challenge.

[2] Another paper, a model of an ad hoc network where nodes communicate with random source–destination pairs. These nodes are assumed to be a mobile. We examine the per-session throughput for applications with loose delay constraints, like this kind of topology changes over the time-scale of packet delivery. Under this assumption, per-user throughput can increase the dramatically when nodes are mobile rather than fixed. This improvement can be achieved by exploiting the form of multiuser diversity via packet relaying. Overall system throughput is maximized by allocating at any time the common channel resource to the user that can best exploit it.

[3] In this paper study about the throughput capacity of hybrid wireless networks. A hybrid network is formed by

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

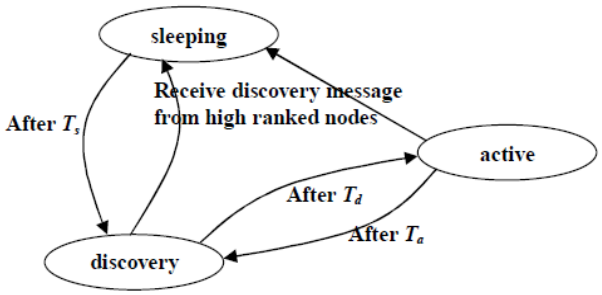
placing sparse network of base stations in an ad hoc network. These base stations are assumed to be connected by the high-bandwidth wired network and act as relays for wireless nodes. They are not data sources or data receivers. The Hybrid networks present a transaction between the traditional cellular networks and pure ad hoc networks in that data may be forwarded in a multi-hop fashion or through the infrastructure.

[4]Another paper proposed how the analysis of the asymptotic capacity of dense mobile ad-hoc networks can be transformed, under the mild assumptions, into a **Maximum Concurrent Flow (MCF)** problem over an associated **Generalized Random Geometric Graph (GRGG).** This methodology allows identifying the scaling laws for a general class of mobile wireless networks. And then to precisely determine under which conditions the mobility of nodes can indeed be exploited to increase the per-node throughput. that a constant per node throughput can be achieved in the case of mobile nodes, by exploiting a novel store-carry-forward the communication paradigm according to which data are physically carried on the nodes as they move around the network area.

III. PROPOSED WORK

In previous work they used CASER protocol it has some advantages such as balanced energy consumption of the entire sensor network so the lifetime of the WSNs can be maximize. And then cost-aware based routing strategies can be applied to address the message delivery requirements. Even though it has some lacks like The adversaries will not able interfere with the proper functioning of the network, such as modifying messages, altering the routing path, or destroying sensor devices and they are able to monitor the traffic in any specific area that is important for them and get all of the transmitted messages in that area.
Here this proposed work is used to overcome these things. By removing few limitations and constraints, we try to present a fundamental. We give a general analysis on the optimal multicast capacity-delay tradeoffs in both the homogeneous and heterogeneous wireless mesh networks.
We assume the mobile wireless network it consists of n nodes, among which ns =ns nodes are selected as sources and nd= n_ destined nodes are chosen for each one. The purpose of this paper is analysis on the multicast capacity-delay tradeoff in wireless mesh networks. Many to many WSNs, shares have high probability to traverse through the same link and to be intercepted by adversaries. In this paper, here they formulate the **Secret-Sharing-Based Multipath routing** as an optimization problem. Our objective aims maximizing both network security and lifetime, subject to the energy constraints using sleep wake state routing protocol with RSA Based Security. Again considering SWS uses the following steps to wake up the guards along the route from S to D:

1. Node S broadcasts the wake-up signal to all its first-hop neighbors (Z, W, n1). The wake-up signal includes identity of both the current sender (S), the next-hop (n1), and the previous-hop (empty for S).



2. Each neighbor of S, after being woken up, decides whether to stay awake or go back to sleep based on the role that it may play on the ongoing communication. If that neighbor is the next-hop (n1), it stays awake to forward the data and to monitor the next-hop from it(n2). If that neighbor is a guard for the next-hop n1over the link n1, n2, it stays awake to monitor the behavior of n1. If the node is a guard of a forwarding node over the previous-hop, it stays awake to detect fabrication by the forwarding node. A node can independently make this determination based on first and second-hop neighbor information. If none of these cases hold, the node goes back to sleep immediately.

3. Node S sends the data packet to n1 following the timing schedule presented

4. Nodes n1, n2, after being woken up continue to stay awake for Tw. After that, it goes back to sleep.

5. n1does the same steps that S did to wake up the next hop (n2), n2's guards (n2, n2) and n1's guards (S, n1, n2).

6. If n1 fails to send the wakeup signal, the guard of n1with the lowest ID sends a two-hop broadcast of the wakeup signal through. If that guard fails, the guard with the next smallest ID sends the signal, and so on. This design ensures that if there is a chain of colluding malicious nodes then all the nodes will be suspected.

IV. EXPREMENTAL RESULT

Wireless sensor network seems inefficient due to its distributed nature becomes alternate to the proposed, in order to determine the optimal route it needs that the base station already has the required information. For the fusion process neural networks are always well suited because neural networks can learn and dynamically adapt to the changing scenarios. Reinforcement learning is the fully distributed and it can adapt quickly to network topology change or any node failure. And It has been used efficiently for finding the optimal path for aggregation. Grouting base routing distributed approach using sleep state switching numbers.

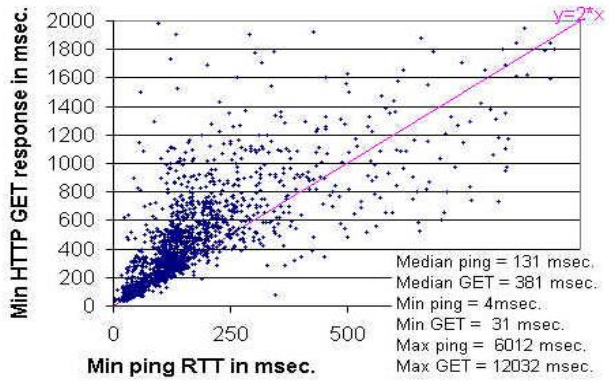
And then weighted average operators to perform the energy efficient flooding-based aggregation has also been propose the system outperforms the previous results .In wireless sensor networks lot of situations demand aggregating data at a central node e.g. monitoring events. For these situations, the centralized approaches like proposed can be used efficiently to know the features of the data are shown in the screen shots

IJARCCE

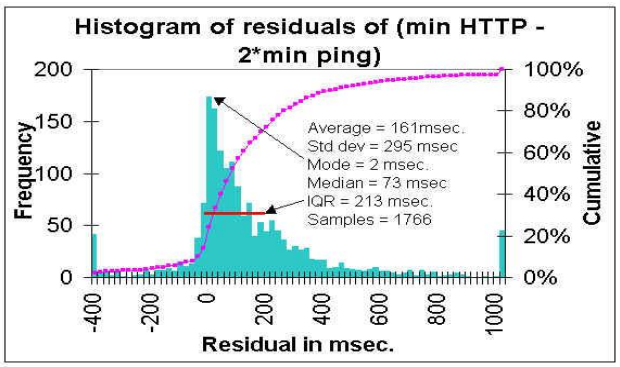
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

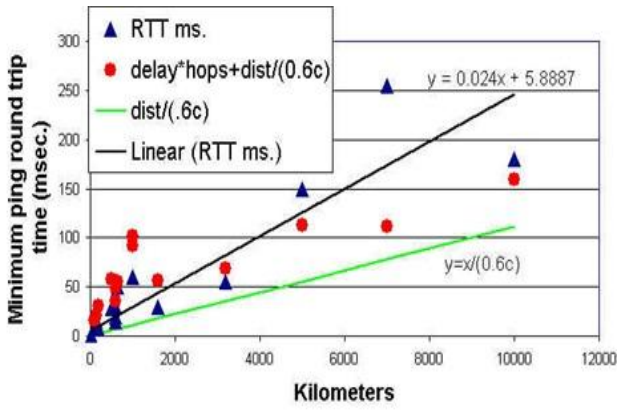
1. **Finding Distance:**



2. Transmission delay:



3. Data Loss Deduction



Roundtrip time versus distance

The above analysis includes calculating percentage of energy conserved in this protocol as well as the previously known protocol. Further time spend by each node in the sense; transmit, off states all are calculated for each node. Based on all the above results, power consumption are calculated for each node. The Total power consumed by single sensor node is calculated based on individual power consumed by the corresponding node in the sense, transmit, off states. Total power consumption of the entire process is calculated based on the total power consumption of the individual nodes. Finally, percentage of energy conserved in this work and previous work is calculated. Theoretical analysis is performed for both static and mobile events.

V. CONCLUSION AND DISCUSSION

Preserving coverage and connectivity in a sensor network has been a problem that has been addressed in the past. However, most of the approaches have assumed the aid of either GPS, or have proposed the use of directional antennas or localization infrastructure. It Given that sensors are envisioned to be light-weight energy constrained devices.

And it may not be desirable to equip them with such additions. In addition, taking advantage of the redundancy of nodes. The scheme can offer energy savings by turning off nodes that may not be required to maintain coverage. Each sensor node conserves its energy by switching between Sense/Receive (or) off states only until it senses an event in its proximity, after which it enters the transmit state to transmit the event information. This work shows that the power saved in each node outperforms the power saved in any other previously known protocols and this work and also shows that it is possible to minimize about 51% of the power and maintain 100% coverage and connectivity. Further, simulation study also proves that it is possible to increase the life time of each sensor network by increasing the number of sensor nodes as well as the security of nodes using RSA algorithm.

VI. FURTHER ENHANCEMENTS

The future work includes providing security to the information passed to the base station. This work does provide security for the information (i.e. the sensed event) passed to the base station. The higher security can be provided to the information which is being transmitted by encrypting it and decrypting it at the base station. The information is encrypted by the sensor node using a shared key (The key that is shared between every sensor node and base station) and only the base station sharing its key can decrypt it. No other sensor nodes or station can decrypt it.

REFERENCES

[1] P. Gupta and P. R. Kumar, "The capacity of wireless networks," IEEE Trans. Inf. Theory, vol. 46, no. 2, pp. 388–404, 2000.
[2] M. Grossglauser and D. N. C. T se, "Mobility increases the capacity of ad hoc wireless networks," IEEE/ACM Trans. Networking, vol. 10, no. 4, pp. 477–486, 2002.
[3] M. Garetto, P. Giaccone, and E. Leonardi, "Capacity scaling in delay tolerant networks with heterogeneous mobile nodes," in ACM MobiHoc 2007, New York, USA, 2007, pp. 41–50.
[4] B. Liu, Z. Liu, and D. Towsley, "On the capacity of hybrid wireless networks," in IEEE Infocom 2003, vol. 2, San Francisco, USA, 2003, pp. 1543–1552.
[5] U. C. Kozat and L. Tassiulas, "Throughput capacity of random ad hoc networks with infrastructure support," in ACM MobiCom 2003, New York, USA, 2003, pp. 55–65.
[6] A. Agarwal and P. R. Kumar, "Capacity bounds for ad hoc and hybrid wireless networks," SIGCOMM Comput.Commun.Rev., vol. 34, no. 3, pp. 71–81, 2004.
[7] X.-Y. Li, "Multicast capacity of wireless ad hoc networks," IEEE/ACM Trans. Networking, vol. 17, no. 3, pp. 950–961, 2009.
[8] X.-Y. Li, Y. Liu, S. Li, and S. Tang, "Multicast capacity of wireless ad hoc networks under Gaussian channel model," IEEE/ACM Trans. Networking, vol. 18, no. 4, pp. 1145–1157, 2010.
[9] X. Mao, X.-Y. Li, and S. Tang, "Multicast capacity for hybrid wireless networks," in ACM MobiHoc 2008, Hong Kong, China, 2008, pp. 189–198.

[10] X.-Y. Li, X. Mao, and S. Tang, "Closing the gap of multicast capacity for hybrid wireless networks," 2009, [Online]. Available: http://www.cs.iit.edu/ xli.
[11] W. Huang, X. Wang, and Q. Zhang, "Capacity scaling in mobile wireless ad hoc network with infrastructure support," in IEEE ICDCS, 2010, Genoa, Italy, 2010, pp. 848–857.
[12] M. J. Neely and E. Modiano, "Capacity and delay tradeoff for ad hoc mobile networks," IEEE Trans. Inf. Theory, vol. 51, no. 6, pp. 1917–1937, 2005.
[13] Mr. K. Kumaravel, V. Renugadevi, Dr. A. Marimuthu, "A Study on Protocols in Wireless Mesh Network", IJCSET, July 2015, vol.6.

BIOGRAPHIES

Dr. K. Kumaravel MCA, M.Phil, CCNA., Ph.D Working as a HOD Department of Computer Science. Dr N.G.P Arts and Science College, Coimbatore, India and Now he is doing Ph.D in Govt Arts & Science College, Coimbatore, he has done his M.Phil in area of networking and post graduate degree in Bharathidasan University, Trichy.

Miss. V. Renugadevi is pursuing M.Phil Research Scholar, Department of Computer Science, Dr N.G.P Arts and Science College, Coimbatore, India.

DOI 10.17148/IJARCCE.2016.5239