2012 International Conference on Information and Network Technology (ICINT 2012)
IPCSIT vol. 37 (2012) © (2012) IACSIT Press, Singapore

Gossip Originated Trusted Leader Selection with Reinforcement in Wireless Mesh Network

Veni devi Gopal [+], Sushma Macha Subramaniam and Divyah Shruthi Jawahar

Department of Information Technology, KCG College of Technology, Chennai, India

Abstract. Wireless Mesh Network is the area where more and more research works are carried on. The mesh network comprises of fixed mesh routers and mobile mesh clients. This paper proposes a unique leader selection algorithm for Wireless Mesh Network. The proposed method is unique in the way that apart from selecting a leader which will help in the co-ordination of the network, it also selects nodes which will help the leader in the coordination process and helps in the reinforcement of the network, once the leader fails. Gossip algorithm is used to share the information among the nodes in the wireless mesh network.

Keywords*:* gossip algorithm, leader selection, wireless mesh network.

1. Introduction

Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are the mobile devices like laptops, cell phones and other wireless devices while the mesh routers are there to forward traffic to and from the gateways which may or may not be connected to the internet. The coverage area of radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. As the number of nodes increase in a network, communication and coordination among the nodes becomes a problem. In such a situation a leader in the network is the best option to coordinate the activities of the network. Once a leader is elected in a network, security can be enhanced. But the main problem with the existing leader election methods is that the complete network completely relies on a single leader, which if fails, will affect the whole network. In this paper, a leader election algorithm is proposed based on gossip algorithm, by which one leader and two other sub-leaders will be selected for the network. Therefore if the leader node fails the other nodes can back up the function of the leader, till the election process is initiated and a new leader is elected. The paper is organized as follows: in Chapter 2 related work done is analyzed in detail. In Chapter 3 a brief review of WMN and its architecture has been presented. Then Chapter 4, the general gossip communication and gossip protocol has been presented. In Chapter 5 we propose an algorithm for electing a leader in WMN. We end up the paper with a conclusion in Chapter 6.

2. Related Work

[12] Proposed a protocol where the leader sensors are selected based on the information which each sensor has gathered. The rest of the sensors will follow the leaders until they have sufficient information on the region of interest and then switch to the standard coverage algorithm.[14] proposed a leader election algorithm in a hierarchy ad hoc network. The idea of selecting vice-president was suggested and it was concluded that the existence of vice-president reduces the time complexity. [13] Proposed two new

[+] Corresponding author. Tel.: + 9443538049.
E-mail address: venidevi@yahoo.com.

algorithms for secure leader election in wireless ad hoc networks. SEFA assumes that all elector-nodes share a single common evaluation algorithm that returns the same value at any electornode when applied to a given candidate-node. The Secure Preference-based Leader Election Algorithm (SPLEA) deals with the case that each elector node has an individual utility function that determines its preference for a given candidate-node. [10] Tried to modify the existing Bully algorithm so that the node with the highest ID becomes the coordinator and if it fails the process is again initiated. The number of messages passed is less in this algorithm. [5] Have presented a leader selection algorithm by modifying Bully and ring algorithm. They have also presented a tree based structure formation and have selected the root node as the leader. [9] Presents a message efficient coordinator election protocol, named ELFA. It uses an underlying routine, called MELFA, to elect cabinet, in very small number of control messages exchange. [1] Proposes a series of local leader selection algorithm based on 2-hop distance neighbors using which they are trying to overcome the effects of selfish nodes in a cluster. [3] Have proposed a leader election for mobile adhoc networks which is highly adaptive for topological changes. They have proposed the algorithm for electing only one leader. [2] Have developed an algorithm for selecting a leader in an anonymous tree based on the preference assigned to the processors. [4] Have implemented an eventual leader abstraction in an infinite arrival model with bounded concurrency. The implementation is based on tracking a property of processes, namely their age, which makes it possible to eventually distinguish between good and bad processes. However, it could always contain bad processes and may never reach a same order on good processes at different processes. [6] Have presented a stable election protocol with a reliable failure detector in completely asynchronous systems. With this approach, the leader election specification states explicitly that progress without violation of safety cannot always be guaranteed. [8], [9] the paper presents a message efficient coordinator election approach. The protocol uses multicast and unicast unlike most of other contemporary protocols that always use message broadcast and Presents a message efficient coordinator election protocol, named ELFA. It uses an underlying routine, called MELFA, to elect cabinet, in very small number of control messages exchange.

3. Architecture and Characteristics of WMN

WMN involves two types of nodes: Mesh routers and Mesh terminal users. The backbone of a WMN is composed of routers which are interconnected and distributed in a mesh way.

WMN can be built with one of the two typical Mesh modes: Mesh mode at the infrastructure end and Mesh mode at the terminal user end. In the former mode, Internet Access Points (IAPs) and terminal users are connected into a wireless closed loop. The IAPs use their routing selection and management functions to select best paths for mobile terminals, while the mobile terminal can, via IAPs, access other networks, such as Wireless Fidelity (Wi-Fi), Worldwide Interoperability for Microwave Access (WiMAX) and sensor networks; hence the compatibility of the network is improved. In the latter mode, terminal users are wirelessly connected into a Point-to-Point (P2P) network. The terminal equipment can run independently without the support of other infrastructure equipment and allow mobile terminals to move at a high rate. Consequently, a broadband network can be quickly constructed. In this mode, the terminal user acts both as a host and a router: on one hand, it runs all related applications; on the other hand, it implements routing protocols and participates in such operations as routing discovery and maintenance.

3.1. WMN architecture

Wireless mesh architecture design is a first step towards providing high-bandwidth Internet access over a specific coverage area. WMNs consist of Mesh Clients (MCs) and Wireless Mesh Routers (WMRs), which relaying each other’s packets in a multi-hop fashion, where mesh routers have minimal mobility and form the Backbone of WMNs (BWMNs). To illustrate more, it is made up of wireless communication nodes, each of which can communicate with other nodes. Mesh architecture breaks the long distance into a series of shorter hops to boost the signal by intermediate nodes. Intermediate nodes not only sustain signal strength, but also forward packages on behalf of other nodes based on their knowledge of the network. Such architecture allows continuous connections and reconfiguration around broken or blocked paths by making forwarding decisions from node to node until the destination is reached. Besides, it provides high-bandwidth Internet access and offers a low cost and flexible deployment. The infrastructure that supports a WMN is a wireless mesh router network, or Backbone Wireless Mesh Network (BWMN). BWMN provides Internet connectivity to MCs in a multi-hop fashion. MCs can access the Internet via BWMN formed by Wireless Mesh Routers (WMRs). BWMN consists of some special WMRs, called as Internet Gateways (IGWs). IGWs act as communication bridges between the Internet and BWMN, and provide Internet accessibility.

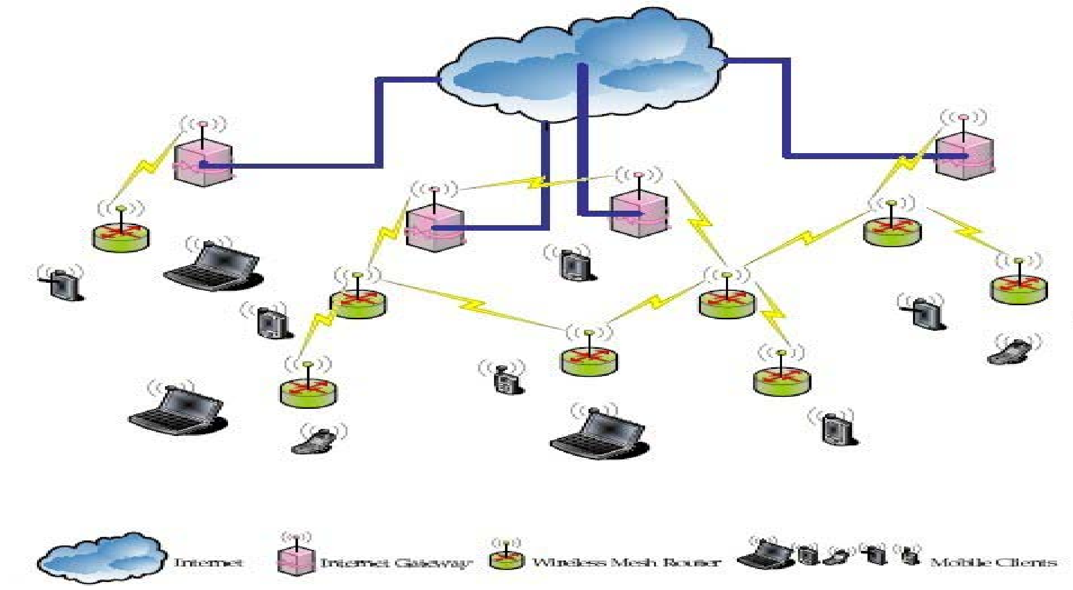

Fig. 1: Wireless Mesh Network

3.2. Components of WMN

There are three types of node in a WMN: WMN client, WMN router, and WMN gateway.

WMN clients are the end-user devices such as: laptops, PDAs, smart phones, etc that can access the network for using applications like email, VoIP, game, location detection, etc. These devices are assumed to be mobile; they have limited power, they may have routing capability, and may or may not be always connected to the network.

WMN routers are in the network to route the network traffic. They cannot terminate nor originate the traffic. The routers have limitation in mobility and they have reliable characteristics. Transmission power consumption in mesh routers is low, for multi-hop communications strategy. Additionally, the Medium Access Control (MAC) protocol in a mesh router supports multiple-channels and multiple interfaces to enable scalability in a multi-hop mesh environment.

WMN gateways are routers with direct access to the wired infrastructure/Internet. Since the gateways in WMNs have multiple interfaces to connect to both wired and wireless networks, they are expensive. Therefore, there are a few number of WMN gateways in the network. Moreover, their placement has a significant impact on the performance of the network.

4. Gossip Protocol

A gossip protocol is a style of computer-to-computer communication protocol inspired by the form of gossip seen in social networks.

Gossip Protocol Types: It is useful to distinguish three prevailing styles of gossip protocol:

● Dissemination protocols (or rumor-mongering protocols). These use gossip to spread information; they basically work by flooding agents in the network, but in a manner that produces bounded worst-case loads:

a) *Event dissemination protocols* use gossip to carry out multicasts. They report events, but the gossip occurs periodically and events don’t actually trigger the gossip. One concern here is the potentially high latency from when the event occurs until it is delivered.

b) Background *data dissemination protocols* continuously gossip about information associated with the participating nodes. Typically, propagation latency isn't a concern, perhaps because the information in question changes slowly or there is no significant penalty for acting upon slightly stale data.

- Anti-entropy protocols for repairing replicated data, which operate by comparing replicas and reconciling differences.

- Protocols that compute aggregates. These compute a network-wide aggregate by sampling information at the nodes in the network and combining the values to arrive at a system-wide value – the largest value for some measurement nodes are making, smallest, etc. The key requirement is that the aggregate must be computable by fixed-size pair wise information exchanges; these typically terminate after a number of rounds of information exchange logarithmic in the system size, by which time an all-to-all information flow pattern will have been established. As a side effect of aggregation, it is possible to solve other kinds of problems using gossip; for example, there is gossip protocols that can arrange the nodes in a gossip overlay into a list sorted by node-id (or some other attribute) in logarithmic time using aggregation-style exchanges of information.

5. Proposed Model

In the proposed algorithm each of the nodes will go through five modes: Sensing mode, voting mode, gossip mode, selection mode and regulation mode.

Sensing mode:

1. Each node has to maintain a trust table.

2. The nodes find out the level of trust of their neighbors, which depends on the number of packets transmitted out of the number of packets received.

Trust = No. of packets transmitted / Number of packets received

3. This value of trust is recorded in the trust table by the nodes along with the id of the immediate neighbor, which are at one hop distance, and the distance of the neighbor.

Voting mode:

4. Once all the nodes have got their trust tables updated, each node forms a set comprising of top three of its neighbors in such a way that their level of trust is more, along with their id.

Gossip mode:

5. Each node transmits its set to its neighbors.

6. The node which receives the set compares the received set with its own set, and forms a new set which will be having the nodes with high level of trust.

Selection mode:

7. Once a node senses that there are no changes in its set and the received set, broadcasts the set.

8. Any node which contradicts with this can reply with its own set in which case the process will be repeated.

9. If no node contradicts then the nodes with the highest level of trust will be announced as the leader.

10. The two other nodes, sub leader nodes, will be the nodes which can replace the leader, in case the leader node fails. These nodes will be used to collect information about the nodes in the network and report to the leader node, periodically.

Regulation mode:

11. The sub leader nodes monitor the functioning of the nodes in the tree and if the trust level of a node goes below a threshold level they will be taken as a malicious node and will be intimated to the leader.

12. The leader intimates this information to the other nodes in the network, so that they select a path excluding the malicious node.

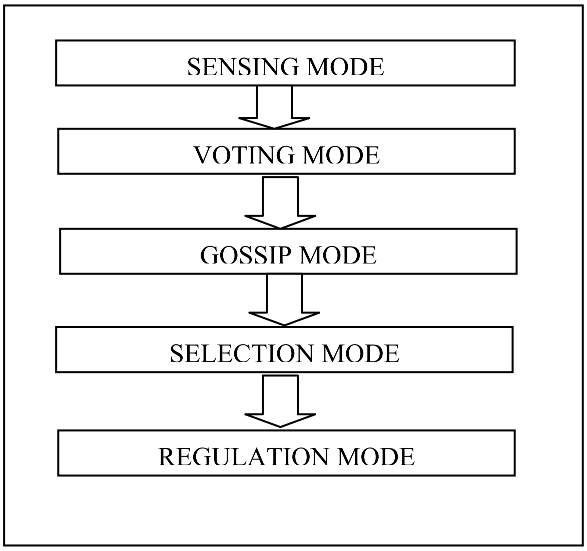

Fig. 2: Example

6. Conclusion

In this paper, we have proposed an algorithm for electing a leader in a wireless mesh network. According to the proposed method each node senses he details about its neighbors, estimates the level of trust of the neighboring node. Based on the level of trust it elects, three nodes as leader and sub-leaders. Then it gossips its voting details with other nodes. The receiving node updates its information based on the received detail. At the end a leader is elected who will coordinate the activities of the network. If the leader node fails, the sub leaders will take control of the network till a new leader is elected. The proposed method avoids the back log that can be caused in case of failure of the leader node, as alternative leaders are there to handle the coordinate the network. In future the proposed method can be implemented and the results can be analyzed.

7. References

[1] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi, And Prabir Bhattacharya, “Mechanism Design-Based Secure Leader Election Model For Intrusion Detection In Manet”, IEEE Transactions On Dependable And Secure Computing, Vol. 8, No. 1, January-February 2011, PP: 89 – 103.

[2] Daniel Fajardo-Delgado, José Alberto Fernández-Zepeda1 and Anu G. Bourgeois, “Randomized Self-Stabilizing Leader Election in Preference-Based Anonymous Trees”, IEEE International symposium on parallel and distributed processing, April 2010, PP: 1 – 8.

[3] Leila Melit, Nadjib Badache, “An Energy Efficient Leader Election Algorithm for Mobile Ad Hoc Networks”, 10th International symposium on Programming and systems, 25-27 April 2011, PP: 54 – 59.

[4] Sara Tucci-Piergiovanni, Roberto Baldoni, “Eventual Leader Election in Infinite Arrival Message-passing System Model with Bounded Concurrency”, European Dependable Computing Conference (EDCC), 2010 European 28-30 April 2010, PP: 127 – 134.

[5] MohammadReza EffatParvar , Nasser Yazdani, Mehdi EffatParvar† , Aresh Dadlani and Ahmad Khonsari, “Improved Algorithms for Leader Election in Distributed Systems”, Second International conference on Computer Engineering and Technololgy, 16-18 April 2010 , PP: V2-6 - V2-10.

[6] Sung-Hoon Park, “A Stable Election Protocol based on an Unreliable Failure Detector in Distributed Systems”, Eighth International Conference on Information Technology, 11-13 April 2011, PP: 979 - 984 .

[7] Hiroyuki Nagataki·, Taichi Fujiit, Yukiko Yamauchi:, Hirotsugu Kakugawat and Toshimitsu Masuzawat, “A kinesthetic-based collaborative learning system for distributed algorithms”, 2010 2nd International Conforence on Education Technology and Computer (ICETC), June 2010, PP: V2-97 - V2-101.

[8] Awadhesh Kumar Singh, Shantanu Sharma, “Message Efficient Leader Finding Algorithm for Mobile Ad Hoc

Networks", Third International conference on Communication systems and networks, 2011, PP: 1 – 6.

[9] Awadhesh Kumar Singh and Shantanu Sharma, "Elite Leader Finding Algorithm for MANETs", 10th International Symposium on Parallel and Distributed Computing, 2011, PP: 125 – 132.

[10] A.Arghavani E.Ahmadi A.T.Haghighat," Improved Bully Election Algorithm in Distributed Systems", Proceedings of the 5th International Conference on IT & Multimedia at UNITEN (ICIMU 2011) Malaysia, November 2011, PP: 1 – 6.

[11] Feng Sen, Qi Bing, Tang Liangrui, "An Improved Energy-Efficient PEGASIS-Based Protocol in Wireless Sensor Networks", Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 2011, Vol:4, PP: 2230 – 2233.

[12] Azwirman Gusrialdi, Risvan Dirza and Sandra Hirche, "Information-Driven Distributed Coverage Algorithms for Mobile Sensor Networks", 2011 International Conference on Networking, Sensing and Control Delft, the Netherlands, 11-13 April 2011, PP: 242 – 247.

[13] Sudarshan Vasudevan, Brian DeCleene, Neil Immerman, Jim Kurose, Don Towsley, "Leader Election Algorithms for Wireless Ad Hoc Networks", Proceedings of DARPA Information Survivability Conference and Exposition, April 2003, Vol 1, PP: 261 – 272.

[14] Gang Zhang, Xiaoyan Kuang, Jing Chen, Yu Zhang, "Design and Implementation of a Leader Election Algorithm in Hierarchy Mobile Ad hoc Network", Proceedings of 2009 4th International Conference on Computer Science & Education, 2009, PP: 263 – 268.