ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

A Detailed Survey on Cluster Based Malicious Node Detection in Wireless Sensor Networks

[1]R. Rohini and [2]R.K. Gnanamurthy

[1]*Faculty of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Namakkal 637 205, India*
[2]*Faculty of Computer Science and Engineering, SKP Engineering College, Tiruvannamalai 606 611, India*

ARTICLE INFO

Article history:
Received 1 November 2015
Accepted 28 November 2015
Available online 18 January 2016

Keywords:
Cluster, Cluster Head, Malicious Node, WSN, Cluster Tree, Routing

ABSTRACT

Wireless Sensor Networks (WSNs) play a vital role in today's real world applications. A primary requirement for the establishment of communication among nodes in Wireless Sensor Networks is that the nodes should cooperate with each other. Each cluster has a cluster head, which is responsible for assisting the general nodes to route the sensed data to the target nodes. The power consumption of a cluster head is higher than that of a general node. But, in the presence of malicious nodes, this requirement may lead to serious security problems, for instance, such nodes may disrupt the routing process. Several cluster based schemes are discussed in this paper. In this paper, we also discuss several literatures not only on improving the network lifetime, but also in the detection of malicious nodes, the detection of which improves the routing process.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: R. Rohini and R.K. Gnanamurthy., A Detailed Survey on Cluster Based Malicious Node Detection in Wireless Sensor Networks. ***Aust. J. Basic & Appl. Sci.,*** *9(35): 343-348, 2015*

INTRODUCTION

WSN refers to a collection of spatially distributed and dedicated sensors for monitoring and recording the physical conditions of an environment and categorizing the collected data at a central location through wireless links. The physical conditions may include pressure, temperature, soil moisture, etc. Each sensor node in Wireless Sensor Network is equipped with a radio transceiver, a microcontroller, an interfacing electronic circuit and an energy source, usually a battery. The energy source in WSN should be handled in an efficient way as it cannot be replaced or recharged if it is placed in harsh or no man environment. In recent days, Wireless Sensor Network (WSN) has drawn many research works predominantly due to its implementation in several applications in different ranges of fields. This includes Environmental Monitoring, Health Monitoring, Military Tracking, Animal Tracking and Monitoring.

In order to support data aggregation through efficient network organization, nodes can be grouped into a number of small sets called clusters. Each cluster has a coordinator, referred to as a cluster head (CH) and several member nodes. The clustering process results in a two-tier hierarchy in which cluster heads (CHs) form the upper tier while member nodes form the lower tier. During cluster formation, it is not sure that all the nodes are becoming a member of any of the cluster. There may be some left-out nodes also in the sensing region after cluster formation which is generally called as individual nodes. Such nodes require higher energy for transmitting the sensed data directly to the sink node. Care is taken to avoid such individual node formation during clustering. The communication between nodes within a cluster is called intra-cluster communication and between nodes of different clusters is called inter-cluster communication as shown in Fig. 1.

Clustering has been extensively studied in the data processing techniques. The clustering approaches developed for this field cannot be implemented directly in WSNs due to its unique operational characteristics. Specifically, WSNs are implemented in an ad hoc manner and comprises of a large number of nodes, which are typically unaware of their locations. Therefore, for WSNs, only distributed clustering protocols are preferred.

Even though the objective of several clustering protocols was to maximize network lifetime, the WSNs operate with the help of battery, which has limited energy. Hence, the clustering method must also concentrate on the detection of malicious nodes which drains the battery power and must avoid such nodes in the data transmission process. In this paper, some literatures which present different clustering

Corresponding Author: R. Rohini, Faculty of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Namakkal 637 205, India
E-mail: rohinir84@gmail.com

methodologies and detection of malicious nodes are discussed.

.

2. Literature Survey:

2.1 Clustering Schemes Based On Various Protocols:

In the approach proposed by Amis *et al*. (2000) the nodes on cluster boundaries are used as gateways to relay data among CHs. This approach is suitable for networks with a fixed transmission power and the protocol allows a cluster to include nodes that are D hops away from the Cluster Head. A node executes 2D iterations before making a decision. This results in a constant number of iterations for convergence. For intra-cluster communication, a cluster member communicates with its CH through multiple hops. Connectivity in this case is a result of the success of cluster formation.

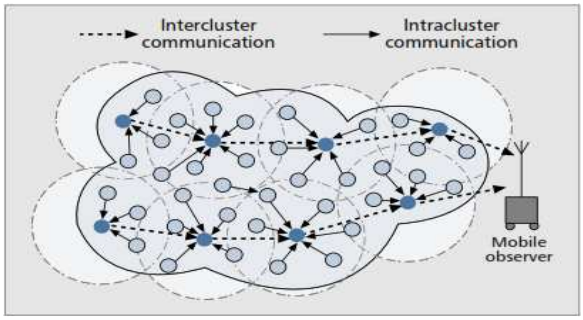

Fig. 1: Illustration of data flow in a clustered network.

In Velmani and Kaarthick (2015), a Velocity Energy-efficient and Link-aware Cluster Tree (VELCT) algorithm for data collection in WSNs was proposed which effectively reduced the problems of mobility, delay, coverage distance, traffic, end-to-end connection and tree intensity. The VELCT algorithm finds the cluster head location and then builds a Data Collection Tree (DCT), in which the data packet from the cluster head is collected and delivers it to the sink by the data collection node. The VELCT algorithm minimized the end-to-end delay, energy exploitation and traffic in CH by implementation of the DCT. The aim of VELCT algorithm is to build a simple tree structure, thereby to reduce the energy usage of the CH and to avoid repeated cluster formations and retain the cluster for a considerable amount of time. Simulation results showed that VELCT algorithm provided better QoS in terms of throughput, energy consumption, end-to-end delay, and network lifetime for mobility-based WSNs.

In Younis *et al*. (2006) the authors focused on distributed clustering approaches designed for large scale sensor networks. Their work discussed some of the basic challenges that prevented the implementation of clustering in recent applications. The scheduling of synchronized intra-cluster and inter-cluster communications, computation of optimal cluster size and optimal frequency determination for CH rotation to maximize the network lifetime are discussed. Several iterative and distributed clustering techniques and their demerits have been discussed in this paper.

Banerjee *et al*. (2001) proposed a centralized technique based on construction of a spanning tree of clusters without the knowledge of node locations, by binding a limitation over the maximum and minimum cluster size. A distributed protocol was also proposed to construct the spanning tree. The efficiency of this approach is limited to large scale networks since all the necessary information is collected and sent twice which consumes more energy. Distributed approaches are more suitable for large-scale networks, where a node joins a cluster or becomes the cluster head depending on the information acquired from its one-hop neighbors.

2.1.1 Iterative Clustering Technique:

In iterative clustering technique, a node waits for a particular occurrence of an event, such as, certain nodes to decide their role (e.g., to become CH or member node) before making a decision. In the Distributed Clustering Algorithm (DCA) (Basagni, S., 1999), a node waits for all its neighbors with higher weights to decide to be CHs or join existing clusters before making a decision. The node with the highest weight among its one-hop neighbors is elected as the CH. If multiple CH announcements are received, the node arbitrates among these CHs using a preference condition (e.g., higher weight wins). If none of the higher-weight neighbors of a node decides to become a CH, then this node decides to become a CH. One of the problems in most of the iterative approaches is that their convergence speed depends on the network diameter (path with the largest number of hops). For example, considering a 2-Dimensional field with *n* deployed nodes, the DCA algorithm requires $O(\sqrt{n})$ iterations for termination process. The worst-case convergence speed can be as slow as (n–1) iterations in a 1-Dimensional setting. The performance of iterative techniques is also highly sensitive to packet losses, i.e. if a node *u* discovers that one of its neighbors *v* has a higher weight, then *u* has to wait for *v* to decide before it makes a decision. The major demerit lies in the fact

that, node *u* has to wait indefinitely for *v* to make a decision if node *v* fails shortly after the neighborhood discovery phase.

2.1.2 Probabilistic Clustering Technique:

The probabilistic approach of node clustering ensures rapid convergence while achieving some significant properties, such as, balanced cluster sizes. It enables every node to independently decide on its role in the clustered network while keeping the message overhead low. Kuhn *et al*. (2004) proposed a probabilistic technique to elect CHs, in which the probability depends on the node degree. The convergence of their proposed technique, which depends on the number of nodes in the network and the node degree, is much faster than iterative techniques. In addition, this approach elects a dominating set of CHs that is asymptotically minimal. Arun Rajesh Sivaraman *et al*. (2015)] have proposed optimization routing using ant colony algorithm.Maximum link utilization was achieved through the multi paths between source and destination nodes in networks. Muticast routing problem was solved by this methodology and it provided maximum utilization ratio. The performance was analyzed using convergence time on different number of nodes in the network. Rejina Parvin *et al*. (2015) have used gravitational search algorithm for reducing energy consumption and increasing the throughput of the wireless sensor networks. Overload of cluster heads were avoided to increase the lifetime of the network. This optimization algorithm was used to form the clusters and provided efficinet routing between source and destination nodes in the clusters. Ramalakshmi *et al*. [26] have developed Optimal Relay Node Placement algorithm for detecting the node failure in the wireless networks. Trust index calcilation parameter was determined to find the number of failure nodes in the cluster.A node with lowest trust degree was computed and this node was declared as failure node in the cluster and these details were delivered to all the nodes in the cluster.

2.1.3 Application-specific clustering:

The LEACH protocol (Heinzelman, W., 2002) is an application-specific clustering protocol, which has been shown to significantly improve the network lifetime. The protocol assumes that all the nodes are available in a single hop and that load distribution is uniform among all nodes. The LEACH protocol allocates a fixed probability to each node so that it can elect itself as a CH. The clustering process proceeds with only one iteration, following which a node decides whether to become a CH or not. Nodes take turns in carrying the role of a CH.

The HEED protocol (Younis, O., S. Fahmy, 2004) considers a multihop network and assumes that all nodes are equally important. A node utilizes its residual energy to probably decide on itself to become a CH. In case of a tie between two CHs, the nodes are selected based on average distance with neighbors or node degree. As a result, uniform distribution of the elected set of CHs across the network is obtained. In HEED protocol, every node generates equal number of iterations. An implementation of HEED in TinyOS, an operating system for Berkeley motes, proved that clustering and data aggregation both doubles the network lifetime.

In Rejina Parvin and Vasanthanayaki (2015), Particle Swarm Optimization (PSO) algorithm is used for cluster formation and Cluster Head selection to reduce the individual/residual node formation. Clustering in the existing Optimized Energy Efficient Routing Protocol results in individual node formation as shown in Fig. 2. For eliminating such individual nodes, the concepts of Particle Swarm Optimization (PSO) are used for cluster formation. Constructing the optimal routing path to transmit the sensed data is another challenging task in WSN. In the proposed system, Gravitational Search Algorithm (GSA) is also used for constructing an optimal routing path to transmit the sensed data to the base station.

PSO encompasses swarm of particles. In general, each and every particle occupies position in the search space. The position's quality is generally being demonstrated by the fitness of each particle which revolves in the search space with a specific velocity. Each particle's velocity is substantially influenced by its best position established in the search space so far and an appropriate solution will be demonstrated by the neighborhood positions. Finally, the swarm will meet the optimal positions.

Vellingiri *et al*. (2014) have developed tree based routing topology in nodes between clusters. The distributed hash tables were used to find the optimized path between the nodes and sink.The route diversity mechanism was utilized in this work to avoid the link failures of the nodes with in the cluster region.Farhad asgari (Farhad asgari, 2014) has construted interfearence free networks using interference cancellation algorithm.The author developed an mathematical model for the elimination of interference between nodes with in the clsuter and between the clusters in the large area wireless networks. The signal-to-noise ratio was computed and based on this, the interference level was determined and poisson point process algorithm was applied on each node to eliminate the interference.

2.1.4 DRINA:

Data Routing for In-Network Aggregation (DRINA) (Sadafal, P.V., R.H. Borhade, 2013) is one which performs Routing Tree construction and finding the shortest path that links all the nodes to all other nodes in the network. The following rules are considered for building the routing Tree. The major steps of DRINA are,

- Constructing the Routing tree

- Electing the Cluster Head (Coordinator)
- Forwarding the sensed data to the Base Station

In this protocol, once base station receives the entire node's information, it allows the nodes to form as clusters.

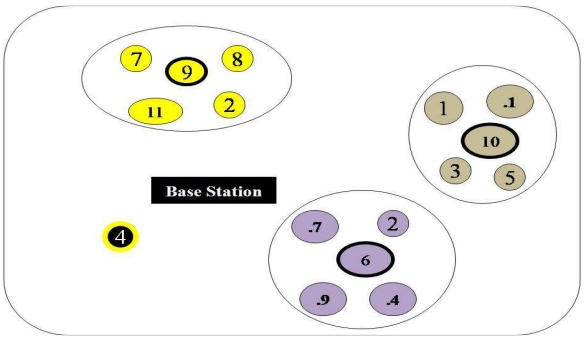

Fig. 2: Cluster formation using PSO algorithm.

2.1.5 OEERP:

Optimized Energy Efficient Routing Protocol (OEERP) is a cluster based routing protocol operating under the principle that makes uniform battery drain of nodes (Chand, K.K., 2012). The function of this protocol can be studied with the help of the following phases:

1) Cluster Formation Phase
2) Information Processing Phase
3) Data Dissemination Phase

In the OEERP method, the individual node formation takes place during cluster formation as shown in Fig. 3. And such individual nodes can become a member of any cluster during next cluster formation and some other node may become as an individual node. Though the percentage of individual nodes varies from one time slot to other, it is a major drawback while considering the network lifetime. Such nodes may die earlier as it has to transmit the sensed data either directly to the Base station or after finding the best next hop.

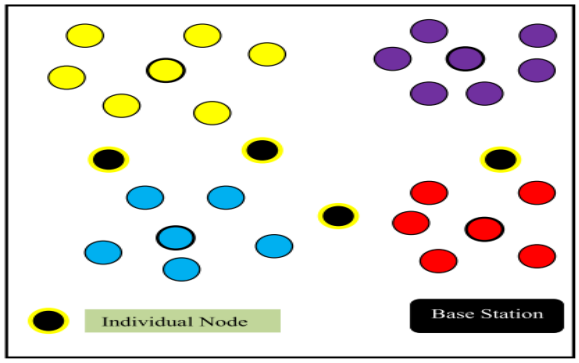

Fig. 3: Cluster formation using OEERP.

2.2 Malicious Node Detection Schemes:

Generally, the malicious node detection mechanisms that have been proposed so far can be classified into Proactive detection schemes and Reactive detection schemes. In the Proactive detection schemes, the method constantly monitors the nearby nodes to detect the malicious node. In these methods, even though there is no malicious node in the network, the resource used for detection purpose is constantly wasted since the overhead of detection is constantly created. Anyhow, one of the advantages of these types of methods is that it can detect the malicious nodes at an earlier stage, thereby avoiding an attack in its initial stage. In the Reactive detection schemes, the method is activated only after the malicious node has been detected by the destination node in terms of significant drop in the packet delivery ratio.

Liu *et al*. (2007) proposed a 2ACK scheme for the detection of routing misbehavior in MANETs. In that scheme, two-hop acknowledgement packets were sent in the opposite direction of the routing path to indicate the successful reception of the data packets. The ratio of data packets received is controlled by parameter acknowledgment ratio. This scheme belongs to proactive clustering type, thereby producing additional routing overhead despite of the existence of malicious nodes.

Cooperative Bait Detection Scheme (CBDS) is presented in Chang *et al*. (2015) that effectively detect the malicious nodes attempting to cause collaborative black hole attacks. The address of an

adjacent node is used as bait destination address to make malicious nodes to send back a reply RREP message, and malicious nodes are detected using a reverse tracing technique. This paper attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism. The CBDS method implements a reverse tracing technique to achieve its goal. The CBDS scheme comprises three steps, namely, the initial bait step, the initial reverse tracing step, and the shifted to reactive defense step. The first two steps belong to initial proactive defense steps, whereas the third step is a reactive defense step. Simulation results showed that CBDS outperformed the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols in terms of packet delivery ratio and routing overhead.

Xue and Nahrstedt (2004) proposed a prevention mechanism called Best-effort Fault Tolerant Routing (BFTR). The BFTR method used end-to-end acknowledgement to monitor the quality of the routing path to be chosen by the destination node, measured in terms of packet delivery ratio and delay. If the behavior of the path deviates from an existing set of routes to determine better routes, the source node uses a new route. One of the drawbacks of BFTR is that, even in the new route malicious nodes may exist and this scheme requires repeated route discovery processes, leading to significant routing overhead.

Most of the proposed algorithms were designed to detect only single malicious node and required high cost and high computational time for detecting cooperative black hole attacks. The TBONE method proposed by Rubin *et al*. (2002) requires specific environments or specific assumptions for its implementation.

Table 1: Comparison survey of different clustering techniques.

Protocol	Year	Objective	Assumptions
Max-Min D-Cluster	2000	D-hop cluster formation, D is a constant	MAC layer provides collision avoidance
Velocity Energy-efficient and Link-aware Cluster-Tree (VELCT)	2015	Reduces the energy consumption of the cluster head	Data Collection Tree (DCT) based on the cluster head location
Distributed Clustering Scheme for Multihop Wireless Networks	2001	Constructs a spanning tree of clusters	A bound on the maximum and minimum cluster size is assumed
Distributed Clustering Algorithm for Ad Hoc Networks	1999	Dominating set of higher weight nodes	Unique, real value weight for every node
Kuhn *et al*.	2004	Minimum dominating set	Three independent communication channels
LEACH	2002	Rapid convergence and maximized network life- time	Single-hop network and uniform load distribution
HEED	2004	Rapid convergence and maximized network life-time	Non-uniform load distribution
Particle Swarm Optimization based Clustering	2015	Eliminates individual node formation and improves overall network lifetime	Each node in WSN is assumed as a particle
Data Routing for In-Network Aggregation (DRINA)	2013	Finds the shortest path	The base station receives all node's information to form clusters
Optimized Energy Efficient Routing Protocol (OEERP)	2012	Avoids individual node formation	Uniform battery drain of nodes
Two-hop acknowledgement scheme	2007	Routing misbehavior detection in MANETs	Additional routing overhead
Cooperative Bait Detection Scheme (CBDS)	2015	Malicious Nodes detection in MANETs	Adjacent node address is used as bait destination address
Best-effort Fault-Tolerant Routing (BFTR)	2004	end-to-end acknowledgements	Repeated route discovery processes
TBONE	2002	Detects cooperative blackhole attacks	Requires specific environments

Conclusion:

In this paper, we have discussed several research works that not only dealt with the problem of increasing network lifetime, but also aimed at the detection mechanism of malicious nodes in Wireless sensor network environment. The detection of malicious nodes in a network automatically reduces the energy consumption of other nodes and unwanted transmissions, thereby increasing the network lifetime. This paper discussed various works of clustering based malicious node detection to protect nodes in WSNs against malicious nodes.

REFERENCES

Amis, A.D., 2000. Max-Min D-Cluster Formation in Wireless Ad Hoc Networks. Proceedings of IEEE INFOCOM, 32–41.

Velmani, R., B. Kaarthick, 2015. An Efficient Cluster-Tree Based Data Collection Scheme for

Large Mobile Wireless Sensor Networks. IEEE Sensors Journal, 15(4): 2377–90.

Younis, O., M. Krunz, 2006. Srinivasan Ramasubramanian. Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges. IEEE Network, 20–5.

Banerjee, S., S. Khuller, 2001. A Clustering Scheme for Hierarchical Control in Multihop Wireless Networks. Proceedings of IEEE INFOCOM, 1028–37.

Basagni, S., 1999. Distributed Clustering Algorithm for Ad Hoc Networks. Proceedings of International Symposium on Parallel Architectures, Algorithms, and Networks, 310–5.

Kuhn, F., T. Moscibroda, R. Wattenhofer, 2004. Initializing Newly Deployed Ad Hoc and Sensor Networks. Proceedings of ACM MOBICOM, 260–74.

Heinzelman, W., A. Chandrakasan, H. Balakrishnan, 2002. An Application Specific Protocol Architecture for Wireless Microsensor Networks. IEEE Trans. Wireless Commun,1(4): 660–70.

Younis, O., S. Fahmy, 2004. Distributed Clustering in Ad Hoc Sensor Networks: A Hybrid, Energy-Efficient Approach. IEEE INFOCOM, Hong Kong, An extended version appeared in IEEE Trans. Mobile Comp, 3(4): 366–79.

Rejina Parvin, J., C. Vasanthanayaki, 2015. Particle Swarm Optimization-Based Clustering by Preventing Residual Nodes in Wireless Sensor Networks. IEEE Sensors Journal, 15(8): 4264–74.

Sadafal, P.V., R.H. Borhade, 2013. Secure clustering algorithm for WSN. Int. J. Emerg. Sci. Eng., 2(2): 1–3.

Chand, K.K., P.V. Bharati, B.S. Ramanjaneyulu, 2012. Optimized energy efficient routing protocol for life-time improvement in wireless sensor networks. Proceedings of Int. Conf. Adv. Eng., Sci. Manage, 345–9.

Baadache, A., A. Belmehdi, 2010. Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks. Intl. J. Comput. Sci. Inf. Security, 7(1).

Marti, S., T.J. Giuli, K. Lai, M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of 6th Annu. Intl. Conf. MobiCom, 255–65.

Vishnu, K., A.J. Paul, 2010. Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks. Int. J. Comput. Appl, 1(22): 28–32.

Liu, K., D. Pramod, K. Varshney, K. Balakrishnan, 20007. An Acknowledgement based approach for the detection of routing misbehavior in MANETs. IEEE Trans. Mobile Comput, 6(5): 536–50.

Deng, H., W. Li, D. Agrawal, 2002. Routing security in wireless ad hoc network. IEEE Commun. Mag, 40(10).

Ramaswamy, S., H. Fu, M. Sreekantaradhya, J. Dixon, K. Nygard, 2003. Prevention of cooperative blackhole attacks in wireless ad hoc networks. Proceedings of Int. Conf. Wireless Networks, 570–5.

Weerasinghe, H., H. Fu, 2007. Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation. Proceedings of IEEE ICC, 362–7.

Chang, J.M., P.C. Tsou, 2015. Isaac Woungang, Han-Chieh Chao, Lai CF. Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach. IEEE Systems Journal, 9(1): 65–75.

Xue, Y., K. Nahrstedt, 2004. Providing fault-tolerant ad hoc routing service in adversarial environments. Wireless Pers. Commun, 29: 367–88.

Kozma, W., L. Lazos, 2009. REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits. Proceedings of WiSec, 103–10.

Wang, W., B. Bhargava, M. Linderman, 2009. Defending against collaborative packet drop attacks on MANETs. Proceedings of 28th IEEE Int. Symp. Reliable Distrib. Syst.

Rubin, I., A. Behzad, R. Zhang, H. Luo, E. Caballero, 2002. TBONE: A mobile-backbone protocol for ad hoc wireless networks. Proceedings of IEEE Aerosp. Conference, 2727–40.

Arun Rajesh Sivaraman, Arun Kumar Sivaraman, M. Lakshmi, 2015. Optimization Routing Using Secure Reverse Multicast Bellman Ford Adhoc Routing and Ant Protocol in Manet. Australian Journal of Basic and Applied Sciences, 9(2): 108-114.

Rejina Parvin and C. Vasanthanayaki, 2015. Mobile Sink Nodes for Energy Efficient Wireless Sensor Networks using Gravitational Search Algorithm. Australian Journal of Basic and Applied Sciences, 9(2): 171-181.

Ramalakshmi, K. and K. Thanushkodi, 2015. Priority Based Prediction of Node Failure and Optimal Relay Node Placement in Wireless Sensor Network. Australian Journal of Basic and Applied Sciences, 9(23): 402-407.

Vellingiri, J., Kumarasamy Saravanan and Ramasamy Asokan, 2014. A Tree Based Routing DHT to Evaluate MAXDISJOINT for MULTIHOP Networks. Australian Journal of Basic and Applied Sciences, 8(18): 356-360.

Farhad asgari, 2014. Interference in wireless ad hoc networks. Australian Journal of Basic and Applied Sciences, 6(9): 353-356.