Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org
Volume 5, Special Issue 2, December (2015)

A Novel Approach for Outlier Detection in MANET's

Renu Popli
Ph. D. Scholar, DCSA, KUK .

Dr. Kanwal Garg
DCSA,KUK

Sahil Batra
GIMT, Kanipla

Abstract – Due to lack of pre-deployed infrastructure, nodes in Mobile Ad-hoc Networks (MANETs) are required to relay data packets for other nodes to enable multi-hop communication between nodes that are not in the radio range with each other. On the other hand, whether for selfish or malicious purpose, a node may not co-operate during the network operations or may interrupt the other node, both of which are recognized as misbehaviors. In short, this problem is an instance of detecting nodes in mobile ad-hoc network, whose behavior is an outlier when compared to others. This paper proposes a novel approach for outlier detection in MANETs using effective data mining technique. Various data mining techniques are suggested for outlier detection .Taking into the consideration of energy constraint the concept of cluster is introduced.

Index Terms – Data mining, Clustering, Outlier detection, MANETs.

This paper is presented at International Conference on Recent Trends in Computer and information Technology Research on 25th& 26th September (2015) conducted by B. S. Anangpuria Instituteof Technology & Management, Village-Alampur, Ballabgarh-Sohna Road,Faridabad.

1. MANET

A Mobile Ad-hoc Network (MANET) [11] is a self-configuring network of mobile devices that are connected by wireless links. In a MANET, each device is willing to serve as a router and share its transmission power with other devices because it is required to forward traffic that is irrelevant to its own interest. Mobile Ad-hoc Networks (MANETs) have a variety of both civilian and military applications, ranging from emergency disaster relief personnel coordinating rescue efforts after a hurricane, earthquake or brush fire to soldiers exchanging information for situational awareness on the battlefield. Other possible applications include mobile healthcare system, real-time traffic alert propagation via vehicular networks, and Cyber-Physical System (CPS).

Security is a key concern in MANETs because the nodes in MANETs are generally more susceptible to various threats than those in the traditional wired networks. From a security perspective, security systems in MANETs differ significantly from those in the traditional wired networks because of the following features of MANETs.

- Open and Error-prone Transmission Medium
- Absence of Utilize Infrastructure
- Rigorous Power Constraint
- Highly Dynamic Network Topology

2. MANET Architecture

Mobile Ad hoc Networks consist of mobile devices communicating over wireless links without any support from a fixed infrastructure. Mobile ad hoc networks are applicable to a wide variety of applications that includes disaster recovery or tactical communication, connection of multiple mobile users in an area at low cost with the use of laptops, portable devices such as PDAs (Personal Digital Assistants), mobile phones, media players, etc. In this network, users can exchange music files, photos, etc, within proximity without connecting to a fixed or Internet infrastructure [13]. A typical MANET architecture is shown in Figure 1.

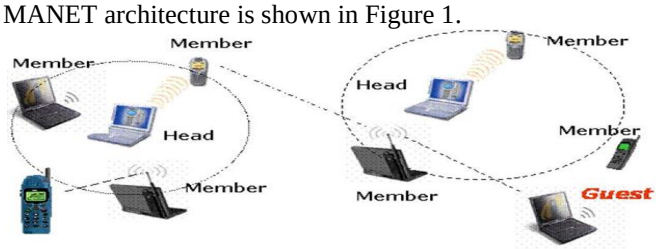

Figure 1: MANET Architecture [7]

3. Introduction To Outlier Detection

Outlier Detection refers to the problem of finding patterns in data that do not conform to expected normal behavior. These anomalous patterns are often referred to as outliers.

3.1. Outlier Detection In MANETs

Outliers in MANETs are generally defined as data points that are very different from the rest of the data with respect to some measure [4, 9]. Outlier Detection can be used for two purposes: either to eliminate outliers and thus potentially reduce them or to expose the outliers for further analysis, such as in intrusion detection, fraud analysis and habitat monitoring for endangered species.

Recently, the topic of Outlier Detection in MANETs has attracted much attention. According to potential sources of outliers as mentioned earlier, the identification of outliers provides data reliability, event reporting, and secure functioning of the network. Specifically, Outlier Detection controls the quality of measured data, improves robustness of the data analysis so that the communication overhead of erroneous data is reduced and the aggregated results are prevented to be affected. The essence of Outlier Detection in MANETs is provided in several real-life applications.

- Environmental Monitoring
- Habitat Monitoring
- Health and Medical Monitoring
- Industrial Monitoring
- Target Tracking
- Surveillance Monitoring

It should be noted that several research topics have been developed for identifying sources of outliers occurred in MANETs. As illustrated in Figure 2, these topics include fault detection, event detection and intrusion detection.

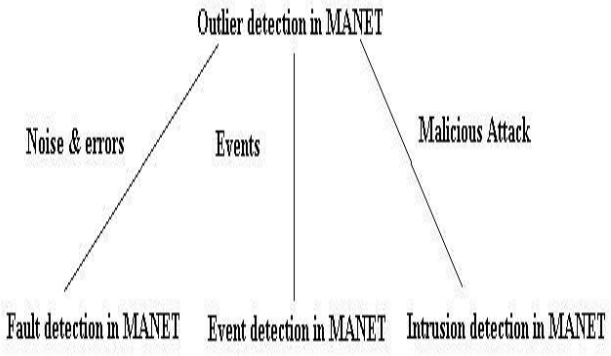

Figure 2: Outlier sources in MANETs and their corresponding detection techniques

3.2. Challenges Of Outlier Detection In MANETs

Extracting useful knowledge from data is not a trivial task. The context of mobile networks and the nature of mobile data make design of an appropriate Outlier Detection technique more challenging. Due to the following reasons, conventional Data Mining techniques used for Outlier Detection might not be suitable for handing data in MANETs.

- Resource Constraints:

The low cost and low quality mobile nodes have stringent constraints in resources, such as energy, memory, computational capacity and communication bandwidth. Most of traditional Data Mining techniques used for Outlier Detection have paid limited attention to reasonable availability of computational resources.

- High Communication Cost:

In MANETs, the majority of the energy is consumed for radio communication rather than computation. For a mobile node, the communication cost is often several orders of magnitude higher than the computation cost.

- Distributed Streaming Data:

Distributed data coming from many different streams may dynamically change. Moreover, the underlying distribution of streaming data may not be known a priori. Furthermore, direct computation of probabilities is difficult.

- Dynamic Network Topology:

Frequent communication failures, mobility and heterogeneity of nodes. A mobile network deployed in unattended environments over extended period of time is susceptible to dynamic network topology and frequent communication failures.

- Large-Scale Deployment:

Deployed mobile networks can have massive size (up to hundreds or even thousands of sensor nodes). The key challenge of traditional Data Mining techniques used for Outlier Detection is to maintain a high detection rate while keeping the false alarm rate low. This requires the construction of an accurate normal profile that represents the normal behavior of mobile data.

Thus, the main challenge faced by Data Mining techniques used for Outlier Detection for MANETs is to satisfy the mining accuracy requirements while maintaining the resource consumption of MANETs to a minimum. In other words the main question is how to process as much data as possible in a decentralized and online fashion while keeping the communication overhead, memory and computational cost low.

3.3. Data Mining Techniques Used For Outlier Detection

Many Data Mining techniques used for Outlier Detection, specifically developed for wireless networks, have emerged. In this section, a technique-based taxonomy framework to categorize these techniques is provided. As illustrated in Figure 3, Data Mining techniques used for Outlier Detection can be categorized into Traditional Approach and New

Generation Approach. Traditional Approach is further divided into Distance Tree Based, Statistical Based and Clustering Based Approach. New Generation Approach is further classified into Nearest Neighbor Based, Neural Network Based and Association Rule Mining Based Approach.

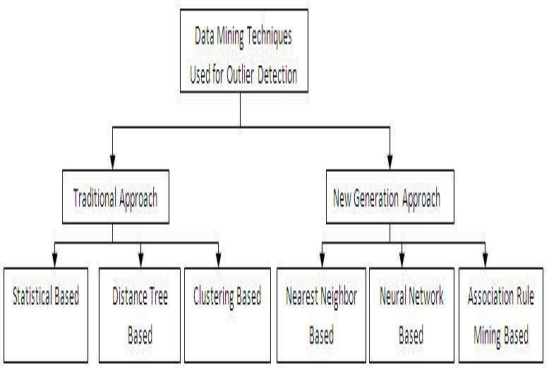

Figure 3: Taxonomy of Data Mining Techniques used for Outlier Detection.

4. LITERATURE SURVEY

In the frequent paragraphs, some of the studies are discussed, which had been previously undertaken in the field of Data Mining Techniques used for Outlier Detection in MANETs, Trust Management in MANETs and Clustering Based Approaches.

4.1. Outlier Detection Using Data Mining In MANETs

Victoria j. Hodge and Jim Austin [10] introduced a survey of contemporary techniques for outlier detection and identified their respective motivations and distinguish their advantages and disadvantages in a comparative review. They provided three fundamental approaches to the problem of outlier detection:

Type 1 – Determine the outliers with no prior knowledge of the data. This is essentially a learning approach analogous to unsupervised clustering.

Type 2 – Model both normality and abnormality. This approach is analogous to supervised classification and requires pre-labelled data, tagged as normal or abnormal.

Type 3 - Model only normality or in a very few cases model abnormality. It is analogous to a semi-supervised recognition or detection task and can be considered semi-supervised as the normal class is taught but the algorithm learns to recognize abnormality. The approach needs pre-classified data but only learns data marked normal.

Branch J et. al. [1] proposed an In-Network Outlier Detection scheme to detect the outliers in wireless sensor networks. In this scheme, all the sensor nodes will first calculate the local outlier(s). Then some messages, which contain the local outlier(s) as well as some other supportive information, will be exchanged amongst all the nodes. The message exchanging process will not halt until all the nodes have the same global view of outlier(s).

Wenjia Li, Anupam Joshi [13] stated an Outlier Detection Framework that aims to reveal the malicious nodes in a MANET environment. Both the Dempster- Shafer Theory of evidence and the Weighted Voting Method applied to combine observation results from multiple nodes. Duc-Son Pham et. al. [3] addressed the Anomaly Detection Problem in large-scale Data Mining applications using Residual Subspace Analysis. The author is specifically concerned with situations where the full data cannot be practically obtained due to physical limitations such as low bandwidth, limited memory, storage, or computing power. Motivated by the recent compressed sensing (CS) theory, a framework is given wherein random projection can be used to obtain compressed data, addressing the scalability challenge.

4.2. Misbehavior Detection And Trust Management Among Nodes In MANETs

Wenjia Li et. al [15] proposed and evaluated a collaborative, gossip-based Outlier Detection algorithm for mobile ad hoc networks. Based on the gossip with neighbours every node maintains its local view and then exchange it and updations are done as required. They[14] analyzed that both the malicious behaviors and the faulty behaviors are generally equally treated as misbehaviors based on which a policy-based malicious peer detection mechanism, is proposed

Pedro B. Velloso, Rafael P. Laufer et. al. [8] proposed a human-based model which builds a trust relationship between nodes in an ad hoc network. The trust is based on previous individual experiences and on the recommendations of others. The Recommendation Exchange Protocol (REP) is presented which allows nodes to exchange recommendations about their neighbors.

Wenjia Li et. Al [12] defined a multi-dimensional trust management framework to better evaluate the trustworthiness of nodes in MANETs. The trustworthiness of a node is judged from different perspectives. The authors also evaluated a [11] Context-Aware Security and Trust framework (CAST) to help better secure MANETs. In CAST, the mobile nodes in MANETs observe and record the abnormal behaviors of their neighbors in a manner similar to existing methods. In contrast to most existing approaches however, each peer also simultaneously collects the context information within which the abnormal behaviors occur. When each peer decides if a node is malicious based on observing abnormal behaviors, it

factors in the context information in a manner specified by a policy.

4.3. Clustering Issues

Dhirendra Kumar Sharma, Chiranjeev Kumar [2] delivered cluster based routing protocols to improve the performance of large-scale networks. A new approach is presented for intra and inter cluster routing in different scenarios. And the proposed algorithm takes the advantages of proactive and reactive routing protocols. For intra and inter cluster routing, proactive and reactive routing concepts are used, respectively. It is assumed that common nodes among the clusters are gateway nodes and act as intermediate nodes. And proposed algorithm enhances the performance of cluster based routing protocol.

N. Gupta, R.K. Singh, M. Shrivastava [5] developed a weight based clustering approach which is based on combined weight metric that takes into account of several system parameters like the mobility, degree difference, transmission range and battery power of the node. One way to support efficient communication between nodes is to partition ad hoc networks into clusters. Various clustering schemes have been proposed to form clusters. Proposed IWCA algorithm can enhance the trust of cluster formation followed by malicious node removal from cluster head or member selection.

5. ISSUES AND CHALLENGES

Data Mining Techniques used for Outlier Detection has great scope in finding out misbehaving nodes in the network. In this research, a few of Data Mining techniques will be used for Outlier Detection to identify outlier node in the mobile ad-hoc environment taking into the consideration of energy constraint in MANETs.

In taking the above issues into considerations, the objectives of this research work will be designing of a mobile network which is divided into various clusters and each cluster should be leaded by cluster head. As nodes in MANETs are limited in energy so to use energy efficiently, cluster heads are used to save all the outlier detection reading found in the cluster. An efficient trust framework can be designed for generating the trust level of every node in the cluster which represents the level of cooperation among nodes. With the establishment of trust it would be possible to detect and isolate misbehaving nodes which acts as outliers. Here objective would be to enable the system to operate despite the presence of misbehavior i.e. how the mobile network make functional for regular nodes when other nodes do not route and forward correctly. All the readings obtained during detection of outlier node at the cluster head node would be then passed to cluster head of other clusters in order to obtain global view of outliers present in the whole network.

6. CONCLUSION

Outlier Detection refers to the problem of finding patterns in data that do not conform to expected normal behavior. Outliers in MANETs are generally defined as data points that are very different from the rest of the data with respect to some measures. Various Data Mining techniques are proposed for detection of outlier data. The main challenge faced by Data Mining Techniques used for Outlier Detection for MANETs is to satisfy the mining accuracy requirements while maintaining the resource consumption of MANETs to a minimum.

REFERENCES

[1]. Branch J, Szymanski B, Wolff R, Giannella C, Kargupta H, "In-Network Outlier Detection In Wireless Sensor Networks.", In Proceedings of the international conference on distributed computing systems (ICDCS),2006.

[2]. Dhirendra Kumar Sharma, Chiranjeev Kumar, "An Efficient Cluster Based Routing Protocol For MANET", 3rd IEEE International Advance Computing Conference (IACC), 2013.

[3]. Duc-Son Pham, Svetha Venkatesh, Mihai Lazarescu, Saha Budhaditya, "Anomaly Detection In Large-Scale Data Stream Networks" Data Mining and Knowledge Discovery, January 2014,Vol. 28, Issue 1, pp. 145-189.

[4]. F. Grubbs, "Procedures For Detecting Outlying Observations In Samples", Technometrics, Vol. 11, No. 1, pp. 1-21, Feb. 1969.

[5]. N. Gupta, R.K. Singh, M. Shrivastava, "Cluster formation through improved weighted clustering algorithm (IWCA) for mobile ad-hoc networks", Tenth International Conference on Wireless and Optical Communications Networks (WOCN), 2013 july,2013,pp. 1-5.

[6]. Nauman Shahid, Ijaz Haider Naqvi,Saad Bin Qaisar, "Characteristics And Classification Of Outlier Detection Techniques For Wireless Sensor Networks in Harsh Environments: A Survey", Springer Science+Business Media Dordrecht, 2013.

[7]. Okeke, S. S. N., Nwabueze, C. A, " Mobile Ad hoc Network (MANET) Architecture And Implementation Analysis", Natural and Applied Sciences Journal 2010, Vol. 11 No. 1.

[8]. Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model", IEEE Transactions on Network and Service Management, vol. 7, no. 3, september 2010.

[9]. V. Barnett and T. Lewis, "Outliers in Statistical Data (3rd edition)", New York, John Wiley and Sons publisher company, 1994.

[10]. Victoria j. Hodge and Jim austin, "A Survey of Outlier Detection Methodologies", Artificial Intelligence Review, springer Vol. 22, Issue 2, pp. 85–126, 2004.

[11]. Wenjia Li, Anupam Joshi, Tim Finin, "CAST: Context-Aware Security And Trust Framework For Mobile Ad-hoc Networks Using Policies", International Conference on Distributed Parallel Databases, Springer, New York 2013.

[12]. Wenjia Li, Anupam Joshi and Tim Finin, "Coping With Node Misbehaviors In Ad-hoc Networks: A Multi- Dimensional Trust Management Approach", Eleventh International Conference on Mobile Data Management, IEEE 2010.

[13]. Wenjia Li, Anupam Joshi, "Outlier Detection In Ad-hoc Networks Using Dempster-shafer Theory", In Proceedings of the Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, MDM 2009, pp. 112–121.

[14]. Wenjia Li, Anupam Joshi and Tim Finin, "Policy-Based Malicious Peer Detection In Ad-hoc Networks.", In Proceedings of 12th IEEE International Conference on Computational Science and Engineering, CSE 2009, Vol. 3, pp. 76–82.

[15]. Wenjia Li, James Parker, Anupam Joshi, "Security Through Collaboration In MANETs." In: Proceedings of 4th International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom 2008, Springer LNICST, Vol. 10, pp. 696–714.

Authors

Renu Popli, received B.tech and M.tech degree from kurukshetra university kurukshetra, in 2008 and 2012 respectively and currently pursuing Ph.D. degree from DCSA, KUK. Her research interests include wireless networks, mobile ad hoc networks and data mining.

Dr. Kanwal Garg, working as Astt. Prof. in DCSA,KUK. He has 14 years of insdustrial/teaching/research experience. His area of expertise is Data mining & ware house, distributed database and parallel database.

Sahil Batra, working as Astt. Prof. in GIMT,Kanipla. He has 4.5 years of teaching/research experience. His area of expertise is wireless networks, mobile ad hoc networks .