

Clustering Based Data Aggregation Method for MANET

Kanika Aggarwal, Dr. Amit Shrivastava

Dept. Computer Science and Engineering, SIRT, Bhopal, INDIA

Abstract— *In today's era of technology and modernization of the organization's work in huge area, there is a need of network which fulfills all the needs of the organization and users to communicate efficiently in huge distributed environment. Explained the sensor nodes which are the event-based systems which provide separate communication networks from the basic version like the sensor networks can have the less energy, power memory and they are of self-organized pattern. In this paper to resolve the issues of more energy consumption and shorter lifetime of MANET, the data aggregation technique will also be explained which provide the aggregation that should be energy-efficient and also provides less delay by compressing the data and hence save the energy.*

Keywords—*component; formatting; style; styling; insert (key words).*

I. INTRODUCTION

Since the last few decades, computer networking was a rebellious domain to enhance. Within the intrusion-detection and prevention-system domain, achievability and chances are boundless, also very risky and there are possibilities of malignant attacks on the networks are high. This is significant for every company to create a security environment which can protect the all authorized access to the system and their resources, also the private information of organizations. Though, full monitor of the security gaps appeared to be not possible currently. Still, it was attempted to find those intrusion attacks also their related activities can be considered as reduce them. This type of domain of the analysis is referred as the intrusion-detection-prevention. Here a detailed overview is presented in this work on the intrusion-detection-systems regarding with the domain by that the traditional field is related.

Within various situations, attacker may not only misuse the application software, rather they also attempt to achieve the illegitimate privileges over the devices of network. Uncontrolled devices of network are the basic origin of the leakage of information within the organizations. The traffic of network is mostly observed to present the unusual change from the usual functioning. Few of these types of peculiarity

are occurred through the malignant attacks of network like viruses or Denial-Of-Service, while the remaining may result in the failure of equipment and the sudden interruptions [1]. Various techniques have been introduced through the companies which performs a significant role to protect the network architecture and the interaction through Internet like by the firewalls or anti-virus packages and the intrusion-detection-systems. Recently available firewalls may not protect against the all the category of the intrusion, whereas the few intrusions may take benefit of the susceptibilities of the computer system [2].

Apparently, for the provided budget of available energy over the network, total numbers of bits which may be forwarded are confined. Also it is required to have ability to send maximum details along with the similar number of bits in air. Mostly, situations are such that data is indicated through these types of redundant bits. As an example, the sequence of the sensing readings along with the similar values may be explained briefly through an average along with the standard-deviation of zero. Since a technique of data aggregation, which may parameterized the description of data-distribution may efficiently decrease the number of the data to be transmitted. As the data-aggregation may decrease the transmissions whereas distributing the details regarding interested events, it is considered as the very efficient location to maintain the requirements of communication and the restraints of energy.

II. MANET

MANETs are strongly susceptible to various kinds of attacks, because of its features like infrastructure less, dynamic topology, susceptible of Terminals, susceptible of channels and the shortage of the strong protection mechanism. These types of mobile terminals may be malignant or selfish in nature. Hence, the deploying of security within the mobile ad-hoc-networks is necessary [3]. The initial protection is done by using the techniques like access-control, authentication, digital signature and encryption through applying the various encryption and verification techniques

to avoid the attacks, though, from the previous experiments may have presented that the encryption and the authentication are utilized as the security protection approaches are not enough.

III. APPLICATION OF DATA AGGREGATION

A. Data aggregation in cluster based

This scheme is designed to provide the data aggregation work which is dependent on the cluster based technique. And this scheme is designed in a manner such that this concept must not match with any other concept and also should provide the same measures and observation for all the different aspects. It never provides different measure for different departments. This scheme is designed for two types of associations.

B. Health-Care-Monitoring

In this type of application there are two ways to implant this concept in medical application. First one provides the tools that are applied externally to the body of human and other one are those that are embedded inside the human body.

C. Bandwidth efficient heterogeneity aware cluster based Data Aggregation (BHCDA)

BHCDA [4] reduces number of transmissions of data packets from sensor terminals to mobile sink. The network model of BHCDA is a connecting graph of different clusters of Wireless Sensor Network (WSN). Each cluster is having heterogeneous terminals and mobile sink. Some terminals from the cluster have high energy are called as Super terminals, some have moderate energy are called as advanced terminals and some are with normal energy are normal terminals. Cluster head (CH) is selected from each cluster. Data Aggregation is done at cluster head (CH) for the packets inside the cluster. These cluster heads (CH) will further acts as a terminals and one of the cluster head (CH) from these CH's, will become aggregator terminal. This aggregator terminal will forward aggregated data to the sink. The aggregation function used in BHCDA is based on correlation of data packets generated by high energy terminals and low energy terminals.

IV. LITERATURE REVIEW

In this work [5] have suggested the energy saving mechanism for developing WSN, which is having the

terminals with high energy and the terminals are allocated within the network closely connected with each other. For the communication within the close network, the required routing methods have been applied for saving the energy of the allocated terminals. In the WSN each terminal get monitored properly and a cluster targeted approach has been developed by accessing the lower common energy abstraction for every terminal.

In this work [6], the concept of wireless sensor networks have been described that every basic element in this network in considered as the terminals which consumes energy while processing, sensing and any type of transmission. By the use of Averaging approach the data get aggregated by aggregating the several sensor terminals of various sources. There are limited resources are available for energy and power within WSN. In this work the REDA approach have been applied with various sensor nodes that detect the single target simultaneously. As the data is collected from the network which is redundant in nature so there is loss of energy while transmitting the data to the sink so the mechanisms to save this energy loss have been described here due to this network's energy get used by the terminals. So to remove this issue the REDA approach have been implemented which follow the grouping of the generated aggregated data and compression of it to remove the redundancy of the generated aggregated data which is get forwarded to the sink without losing its accuracy. Security and the energy-efficiency are the two more issues that have also been found in WSNs.

[7] Within this work suggested a mechanism by using the data aggregation method to optimize the usage of energy within the multi-hop WSN of every sensor terminals. In this work intermediate terminals have worked for quickly modified data and for constant data also. After applying efficient-energy aware routing-and-data-aggregation within the multi-hop WSN approach, the result of simulation presents that there is a decrease in the consumption of network energy. Hence this approach decreases the need of network by preventing the transmission of redundant bits. Due to this there is a possibility in future to apply this system on the real-time networks. In this aspect study on huge networks and different types of topologies have also been done efficiently. This feature made this approach to be practical to be used effectively within new terminals.

V. PROPOSED WORK

There is various aspect of the MANET. To make MANET perform better many aspects could play an effective role. Data aggregation is one of those aspect which can make use of MANET more efficient. Proposed architecture of data aggregation is based on clustering and describe in fig 1.

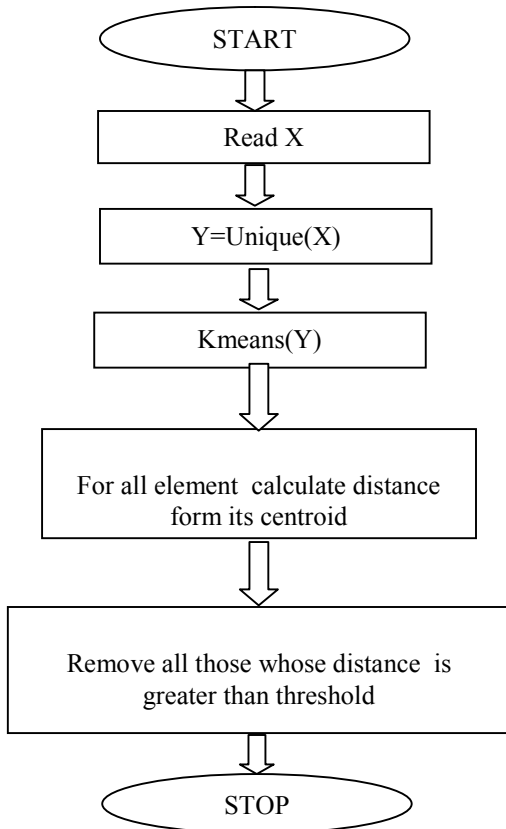


Fig 1: Proposed Work Architecture

Input: Original Dataset
 Output: Aggregated Data Set
 Procedure:

1. Read syslog file in X
2. Remove reapeating Rows in X → Y
3. kmeans(Y,2) → X1,X2
 // Cluster data in 2 cluster X1,X2
4. for i=1 to no_rows_in Y
 Di=dist(Cj,Xji);
 // Calculate distance of each element //from its element
 End for
5. Remove those element having Di>threshold → Data;

From fig 1 and 2, it is clearly shown that how the propose work is doing. Under this proposed work first of all the duplicate data has been removed. In the second step the clustering is done on the rest of the data. After performing this clustering the distance is calculate and based on this distance again data is aggregated. All the process is clearly shown in both figures.

VI. SIMULATION AND RESULT ANALYSIS

There are three phases of the simulation and results analysis. These are as follows:

1. Dataset
2. System
3. Result

Dataset: Dataset is Kyoto dataset. It is a collection of web log data from 2006 to 2010 [9]. It consists of 24 statistical features; 14 conventional features and 10 additional features. Among them, the first 14 features were extracted based on KDD Cup 99 data set, which is a very popular and widely used performance evaluation data in intrusion detection research field [10].

System: Used system for performing the experiments contents Core 2 Duo along with 4 GB RAM. It also has 32 bits Windows 7 Operating System.

Results: Table I and II show the Aggregation ratio with execution time.

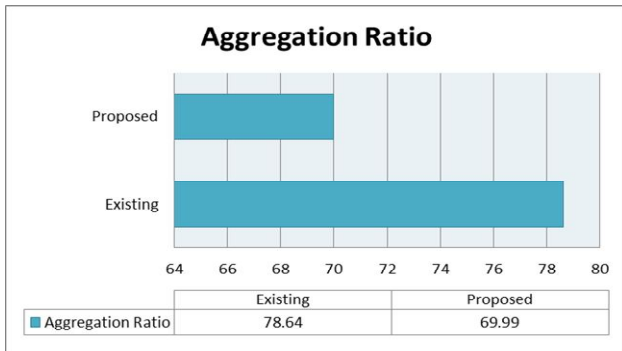
Aggregation Ratio: It is a quantity which shows in percentage of aggregation of data with respect to original data.

Table I: Aggregation Ratio

	Existing	Proposed
Aggregation Ratio	78.64	69.99

Table II: Execution Time

	Existing	Proposed
Execution Time	23.023	0.278



Graph 1: Aggregation Ratio



Graph 2: Execution Time

From TABLE I & II along with graph 1 & 2, it is clearly represent the performance measures of suggested work of DATA_AGGREGATION approach .

VII. CONCLUSION

The main consideration of this work is energy issue within MANET. Computational cost is also another main aspect in this work during the processing of any information. With the decrease of the computational cost the efficiency of the network get raised. Less sized data is efficient for maintaining the efficiency of energy in network. This current work is done for the same and achieved higher data aggregation which makes network working more efficiently.

REFERENCES

[1] Chundong Wang, Quancai Deng, Qing Chang, Hua Zhang and Huaibin Wang “ A New Intrusion Detection System Based on Protocol Acknowledgement” IEEE 2010
 [2] Anuradha and Anita Singhrova A Host Based Intrusion Detection System for DDoS Attack in WLAN IEEE International Conference on Computer & Communication Technology (ICCC)-2011

[3] Rajesh D. Wagh, Swapnil D. Kurhe, Saurabh R. Dahake, ” An Overview on Intrusion Detection in Manet”, International Journal on Computer Science and Engineering (IJCSSE), Vol. 7 No.5 May 2015.
 [4] Dnyaneshwar Mantri, Neeli Rashmi Prasad, Ramjee Prasad, “BHCDA: Bandwidth Efficient Heterogeneity aware Cluster based Data Aggregation for Wireless Sensor Network,” ICRTIT 2011, 978-1-4673-6217-7/13 2013 IEEE.
 [5] Zahra Beiranvand and Ahmad Patooghy, ”ILEACH: An Efficient Routing Algorithm to Improve Performance & to Reduce Energy Consumption in Wireless Sensor Networks”, 2013 5 th Conference on Information and Knowledge Technology (IKT), 978-1-4673- 6490-4/13 ©2013 IEEE.
 [6] Yogita hukre, nikita v. mahajan, "Data Aggregation Techniques Of Wireless Sensor Network Increasing Network Lifetime Using Readable", Proceedings of 19 th IRF International Conference, 25th January 2015, Chennai, India, ISBN: 978-93-84209-84-1.
 [7] Kiruthika.A , Sugandhi.N , "The Efficient Energy Aware Routing and Data Aggregation in Multi-Hop Wireless Sensor Network", International Journal of Innovative Research in Science, Engineering and Technology , Vol. 4, Issue 1, January 2015.
 [8] Prakashgoud Patil, Umakant Kulkarnim, "Delay Efficient Distributed Data Aggregation Algorithm in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 69– No.1, May 2013.
 [9] http://www.takakura.com/Kyoto_data/ 2010.
 [10] The third international knowledge discovery and data mining tools competition dataset KDD99-Cup <http://kdd.ics.uc i.edu/databases/kddcup99/kddcup99.html>, 1999.