International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-2, Issue-4, July- 2014

Detection & Deletion of DDOS Attacks Using Multi-clustering Algorithm

Meera A R, Jismy K Jose

***Abstract*-Wireless sensor networks are mostly vulnerable to attacks. It's difficult to find /track attacker due to mobility. Indeed, the numbers of new attacks as well as their sophistication are continuously increasing. Diametrically opposite strategy has been studied in the last few years such as unsupervised anomaly detection (UAD). UAD uses data mining techniques to extract patterns and uncover similar structures "hidden" in unlabeled traffic or unknown nature (attack or normal operation traffic), without relying on Digital signatures or baseline traffic profiles. Based on the observation that attacks, particularly the most difficult ones to detect are contained in a small fraction of traffic flows with respect to normal operation traffic so we propose a paramount advantage of unsupervised, knowledge-independent detection algorithms based on clustering. The main aim is to combine the clustering results provided by multiple independent partitions of the same set of flows and filtering out biased groupings. We focus on the detection and characterization of standard and well-known attacks, which facilitates the interpretation of results. Denial of service (DOS), distributed DOS (DDOS), network scans, and worm propagation are examples of such standard network attacks. The approach can easily be generalized to detect other kinds of anomalies and attacks.**

***Index Terms* — Unsupervised anomaly detection (UAD), Denial of service (DOS), Distributed DOS (DDOS)**

I. INTRODUCTION

A wireless sensor network (WSN) is a collection of sensors with limited resources that Collaborate to achieve a common goal. It consists of spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location.

Manuscript received July 08, 2014.
Meera A R, Assistant Professor,Cochin University College of Engineering Kuttanadu, Pulincunoo, India. (e-mail: ar.meera@gmail.com).
Jismy K Jose, Assistant Professor,Cochin University College of Engineering Kuttanadu, Pulincunoo, India. (e-mail: jismy89@gmail.com).

The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Area monitoring

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors to detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.

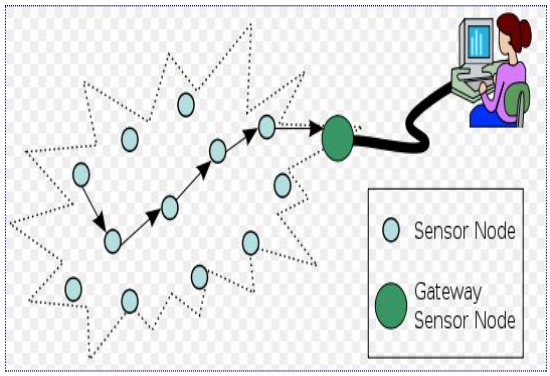

Figure 1.1 Wireless Sensor Network

Air pollution monitoring

Wireless sensor networks have been deployed in several cities (Stockholm, London or Brisbane) to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad-hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas.

Forest fires detection

A network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced by fires in the trees or vegetation. The early detection is crucial for a successful action of the firefighters; thanks to Wireless Sensor Networks, the

fire brigade will be able to know when a fire is started and how it is spreading.

Greenhouse monitoring

Wireless sensor networks are also used to control the temperature and humidity levels inside commercial greenhouses. When the temperature and humidity drops below specific levels, the greenhouse manager must be notified via e-mail or cell phone text message, or host systems can trigger misting systems, open vents, turn on fans, or control a wide variety of system responses.

Landslide detection

A landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide. And through the data gathered it may be possible to know the occurrence of landslides long before it actually happens.

Industrial monitoring

Machine health monitoring

Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors.

Water/wastewater monitoring

There are many opportunities for using wireless sensor networks within the water/wastewater industries. Facilities not wired for power or data transmission can be monitored using industrial wireless I/O pollution control board.

Agriculture

Using wireless sensor networks within the agricultural industry is increasingly common; using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured and wirelessly transmitted back to a central control center for billing. Irrigation automation enables more efficient water use and reduces waste.

Structural monitoring

Wireless sensors can be used to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc... enabling Engineering practices to monitor assets remotely without the need for costly site visits, as well as having the advantage of daily data, whereas traditionally this data was collected weekly or monthly, using physical site visits, involving either road or rail closure in some cases. It is also far more accurate than any visual inspection that would be carried out.

Wireless sensor networks are mostly vulnerable to attacks. It's difficult to find /track attacker due to mobility. Indeed, the numbers of new attacks as well as their sophistication are continuously increasing. Diametrically opposite strategy has been studied in the last few years such as unsupervised anomaly detection (UAD). UAD[4] uses data mining techniques to extract patterns and uncover similar structures "hidden" in unlabeled traffic or unknown nature (attack or normal operation traffic), without relying on Digital signatures or baseline traffic profiles.

The unsupervised detection of network attacks are based on clustering techniques and outliers detection. Different clustering algorithms produce different partitions of data, and even the same clustering algorithm provides different results when using different initializations or different algorithm parameters. This is in fact one of the major drawbacks in current cluster analysis techniques: the lack of robustness.

II. NETWORK ATTACK

We focus on the detection and characterization of standard and well-known attacks, which facilitates the interpretation of results. Denial of service (DOS), distributed DOS (DDOS), network scans, and worm propagation are examples of such standard network attacks. The approach can easily be generalized to detect other kinds of anomalies and attacks. Network traffic monitoring has become an essential means for detection of network attacks. Wireless sensor networks are mostly vulnerable to attacks. It's difficult to find /track attacker due to mobility. Indeed, the numbers of new attacks as well as their sophistication are continuously increasing.

Different approaches studied are Signature-based detection systems, Supervised anomaly detection, unsupervised anomaly detection [4]. Signature-based detection systems are based on extensive knowledge of the particular characteristics of each attack, referred to as its signature. The signature based detection detect what is known. It does not detect any unknown signatures. Supervised anomaly detection relies on the existence of some kind of baseline profile with special and complicated algorithms such a watchdog or sign based detection system for normal operation that deviate from normal traffic. The supervised anomaly detection detects what is different from what is known. Detect anomalies [8] as traffic events that deviate from normal traffic. It requires strong knowledge about what is seen "normally" that is about the basic behavior. It is difficult to maintain up to date normal operation profile.

Unsupervised Anomaly Detection [9] uses data mining techniques to extract patterns and uncover similar structures "hidden" in unlabeled traffic of unknown nature. The unsupervised detection of network attacks is

based on clustering techniques and outliers detection. Different clustering algorithms produce different partitions of data, and even the same clustering algorithm provides different results when using different initializations or different algorithm parameters. This is in fact one of the major drawbacks in current cluster analysis techniques: the lack of robustness.

III. PROPOSED SYSTEM

An alternative clustering approach is presented to perform robust unsupervised detection of attacks. The main idea is to combine the clustering results provided by multiple independent partitions of the same set of flow. The combination of multiple evidence [6] on flow groupings adds robustness to the process of separating malicious from normal operation traffic. Automatic characterization and updation of attacks is used to find out the variation of flow.

To show the concept on robust unsupervised detection [1] approach a complete system is developed to detect network attacks without any kind of `signatures or previous knowledge of context traffic. Information provided by the multi-clustering[1],[6] approach is to characterize an identified group of malicious flows, automatically producing easy-to-interpret signatures of the attack. These signatures provide useful information on the nature of the attack, and can be directly exported to any security device (e.g., IDS, IPS, firewall) to easily detect its occurrence in the future.

Examples of the features

Table 3.1 Different features used to detect and characterize standard network attacks

Features	Description
NSrcs	Number of sources
NDsts	Number of destinations
nSrcs/ nDsts	Ratio of nSrcs to nDsts
NSrcPorts	Number of different source ports
NDstsPorts	Number of different destination ports
nPkt/sec	Number of packets per second
nPkts/nDst	Number of packets per destination
nICMP/nPkts	Fraction of ICMP packets
nSYN/nPkts	Fraction of SYN packets

The list of features in the Table 3.1 includes standard and very basic traffic descriptors, which permits to characterize detected anomalies[8] in easy-to-interpret terms. The features are good enough to detect and characterize standard network attacks such as DoS, DDoS, and network scans.

IV. IMPLEMENTATION

A. Node Creation

Create Wireless Sensor Network . Then selecting source and destination. Requesting packet from source to destination. Reply packet is sent from destination to source via shortest path. Packets are transferred via shortest path. Analysing the performance of normal data traffic.

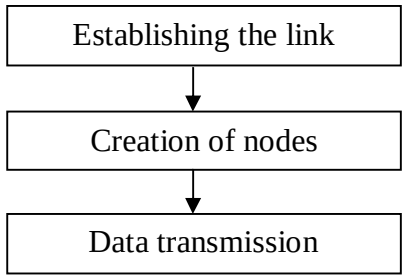

Figure 4.1: Creation of wireless network

B. Traffic Generation

In the fig.4.2, Topology for more number of nodes are shown. Transmission of packets between the nodes is done. Parameters such as throughput, end to end delay, packet delivery ratio are calculated.

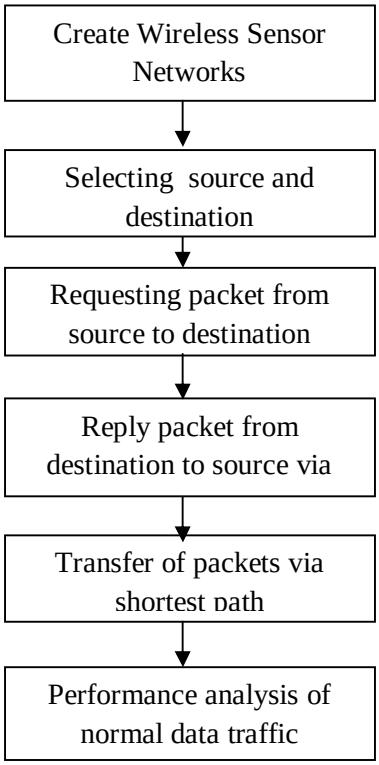

Figure 4.2: Topology of more nodes for traffic generation

C. Network Attack

In the fig.4.3,Topology for more number of nodes are shown. Transmission of packets between the nodes with implementing DDOS(Distributed Denial of Service) attack is done. Parameters such as throughput, end to end delay , packet delivery ratio are calculated .

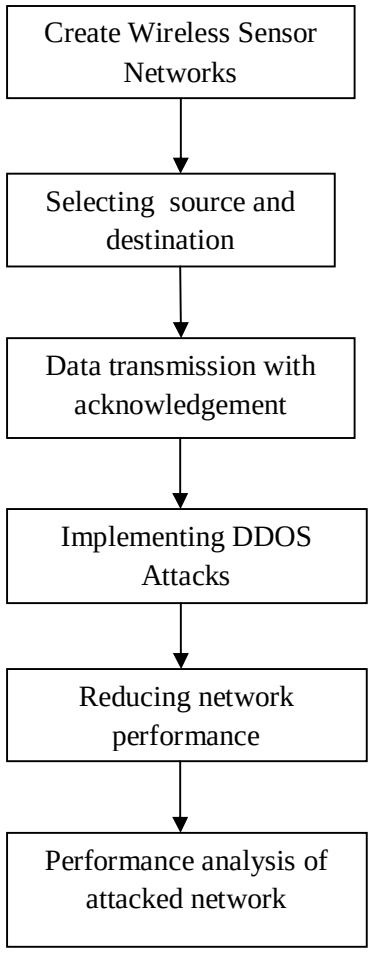

Figure 4.3:Implementing DDOS attack

D. Unsupervised Detection With Signal Strength Analysis technique

In the figure 4.4, Topology of wireless sensor network with more number of nodes. Transfer of packets between the nodes. Unsupervised detection (by forming clustering methods) technique[1] is used to detect malicious nodes.Detection of DDOS attack and deletion of malicious node is done using Robust Multiclustering based detection algorithm with Signal Strength Analysing technique. Transmission rate and overall traffic is calculated.

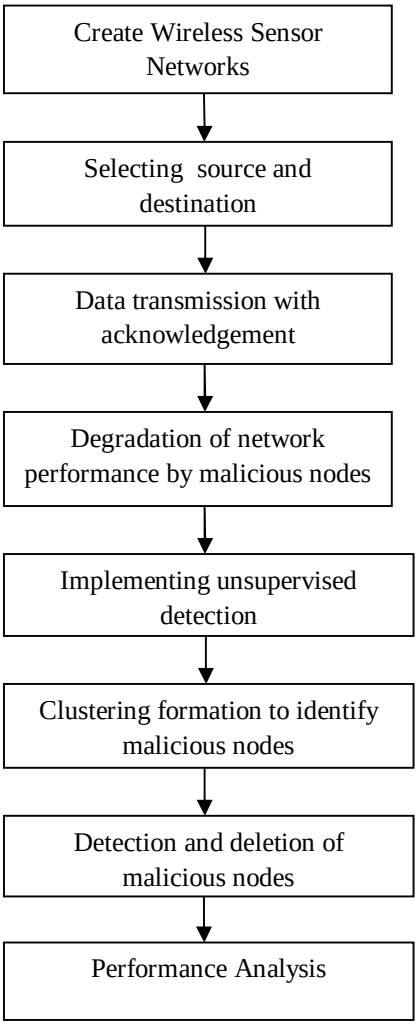

Figure 4.4: Detection and deletion of malicious nodes using unsupervised detection technique

E. Access Point Analysis With Network Traffic Level

In the figure 4.5,topology for more number of nodes with access point.Access point analysis of traffic level to detect malicious nodes. Sharinginformation of malicious nodes to other nodes and stopping communicationwith malicious nodes.

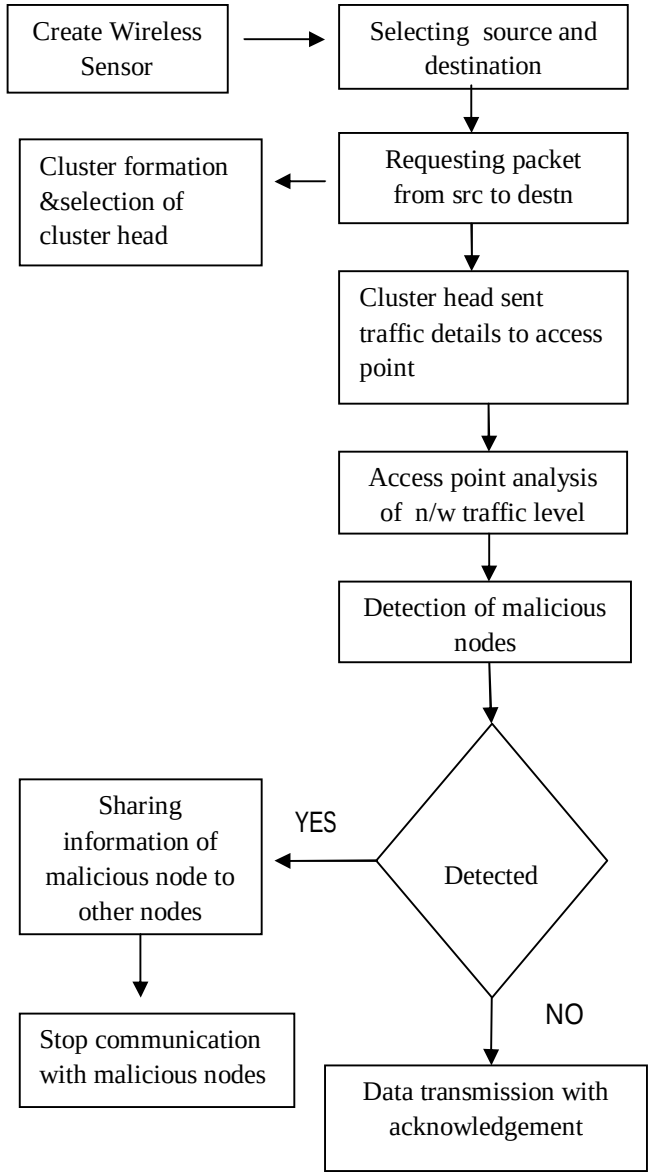

Figure 4.5: Access point analysis

V. CONCLUSION

In this paper, study of malicious nodes is evaluated and unsupervised detection with clustering formation is implied to find the characteristics of attacks. Malicious nodes are avoided to safeguard the network performance. Although malicious nodes are detected accordance with changes in one of the parameter, the adversary node can make changes in other parameters and it may affect the performance of network. Acquired information of traffic level and data rate of normal nodes are sent to access point. Access point analysis thenetwork traffic level and detects the attacker. Access point sentattacker

information to other nodes to avoid attacker and to stop communication. Thereby,network can be protected from malicious nodes and network will be safe.

REFERENCES

[1] Pedro Casas, Johan Mazel, and Philippe Owezarski, CNRS and Universite de Toulouse, "Knowledge-Independent Traffic Monitoring: Unsupervised detection Of Network Attacks," IEEE Network.January/February 2012

[2] G. Androulidakis, V. Chatzigiannakis, and S. Papavassiliou, "Network Anomaly Detection and Classification via Opportunistic Sampling," IEEE Network vol. 23, no. 1, 2009.

[3] K. Cho, K. Mitsuya, and A. Kato, "Traffic Data Repository at the WIDE Project," Proc. USENIX Annual Technical Conf., 2000

[4] E. Eskin et al., "A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data," Applications of Data Mining in Computer Security, Kluwer Publisher, 2002.

[5] G. Fernandes and P. Owezarski,"Automated Classification of Network Traffic Anomalies," Proc. 5th Int'l. ICST Conf. Security and Privacy in Communication Networks, 2009

[6] A. Fred and A. K. Jain, "Combining Multiple Clusterings Using Evidence Accumulation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol.27, no. 6, 2005, pp. 835–50.

[7] A. K. Jain, "Data Clustering: 50 Years Beyond K-Means," Pattern Recognition
Letters, vol. 31, no. 8, 2010, pp. 651–66.

[8] A. Lakhina, M. Crovella, and C. Diot,"Mining Anomalies Using Traffic Feature Distributions," Proc. ACM SIGCOMM, 2005.

[9] K. Leung and C. Leckie, "Unsupervised Anomaly Detection in Network Intrusion Detection Using Clustering," Proc. 28th ACSC, 2005.

[10] H. Ringberg et al., "Sensitivity of PCA for Traffic Anomaly Detection," Proc.ACM SIGMETRICS, 2007.

Meera A R is working as a Assistant Professor in Cochin University College of Engineering Kuttanadu, Pulincunoo, Alappuzha under Cochin University of Science & Technology. She did her Master's Degree in Software Engineering & Bachelor's Degree in Computer Engineering from Cochin University of Science & Technology. She has 14 years experience in teaching. Her areas of interests include Software Engineering, Operating System, Advanced Architecture, Security in Computing, Cryptography and networking.

Jismy K Jose is working as a Lecturer in Cochin University College of Engineering Kuttanadu, Pulincunoo, Alappuzha under Cochin University of Science & Technology. She did her Master's Degree & Bachelor's Degree in Computer Science& Engineering from Anna University, Chennai. She has presented papers in National & International conferences. Her areas of interests include Network Security, Datamining, SoftwareEngineering