An Approach to Hybrid Anomaly Detection using K-Means Clustering in WSN

Mohammad Wazid
Department of CSE
Graphic Era University
Dehradun, India
wazidkec2005@gmail.com

Avita Katal
Department of CSE
Graphic Era University
Dehradun, India
avita207@gmail.com

Roshan Singh Sachan
Department of CSE
Graphic Era University
Dehradun, India
rsachan28@gmail.com

R H Goudar
Department of CSE
Graphic Era University
Dehradun, India
rhgoudar@gmail.com

***Abstract*— Security is a biggest concern in Wireless Sensor Networks (WSNs) especially for the ones which are deployed for military applications and monitoring. They are prone to various attacks which degrades the network performance very rapidly. Sometimes multiple attacks are launched at the same time in the network. In this situation it is very hard to find out which kind of anomaly is activated in the network. In this paper we have done the analysis of the network data set which consists of Traffic data and End to end Delay data in order to find the anomaly. The data set is clustered using Weka tool. By analyzing the clusters computed by Weka and given as an output, we have concluded that two anomalies exist in the network one causing Misdirection attack and second causing Blackhole attack.**

Index Terms— Hybrid Anomalies; Misdirection; Blackhole; K-Means Clustering.

I. INTRODUCTION

WSN can be easily attacked by enemies which causes information loss along with large energy expenditure. Therefore, securing the links is important in designing a sensor network. In this paper we have done the clustering of data set of various anomalies which exist in the sensor network. On the basis of computed clusters we have found that two kinds of anomalies are exist in the network i.e. Misdirection Attack and Blackhole Attack.

The rest of the paper is organized as: Section II of this paper includes the related work done by various authors in this field. Section III contains the problem definition followed by the related terminology being defined in Section IV. The Methodology and the Experiment Design of the work done is explained in Section V and VI respectively. Section VII contains the key findings of the work followed by the conclusion in Section in VIII.

II. RELATED WORK

In paper [1] a hybrid detection framework that depends on data mining classification and clustering techniques is proposed. Random forests classification algorithm is used in order to detect misuse by building intrusion patterns from training dataset. These patterns are then matched with network connections to detect network intrusions. K-means clustering algorithm is used to detect novel intrusions by clustering the network connections for anomaly detection. In paper [2] authors have done a topological analysis of WSN in the presence of misdirection attack and an algorithm for the prediction of delay and throughput prediction is discussed.WSN performs better for tree network topology as compared to mesh topology was the key finding of the paper. In paper [3] Anomaly traffic detection system based on the Entropy of network features and Support Vector Machine (SVM) are compared. A hybrid technique that is a combination of both entropy of network features and support vector machines is compared with the individual methods. In paper [4] hybrid anomaly-based intrusion detection method is proposed that is based on these two methods. These methods are trained in supervised way. The authors have used following additional techniques to improve the performance of proposed approach: First, a feature selection technique using the entropy of features is used for extracting optimized information from KDD data set and second, a novel method is proposed to combine the results of these two learning based methods. In paper [5] the attempt has been made to apply hybrid learning approach by combining k-Medoids based clustering technique followed by Naïve Bayes classification technique. Because of the fact that k-Medoids clustering techniques represent the real world scenario of data distribution, the proposed enhanced approach will group the whole data into corresponding clusters more accurately than k-Means such that it results in a better classification. An experiment is carried out in order to evaluate performance, accuracy, detection rate and false positive rate of the classification scheme. In paper [6] a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes is proposed. Multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node are being used. The results obtained indicate that trust-based geographic routing approaches the ideal performance level achievable by flooding-based routing in message delivery ratio and message delay without incurring substantial message overhead. In paper [7] a new frame work based on a hybrid intrusion detection system for known and unknown attacks in an efficient way has been proposed. This frame work has the ability to detect intrusion in real time environment from the link layer. In paper [8] a hybrid IDS is being proposed which uses the signature and anomaly information together. The proposed algorithm first explore those traffic features which are changing during an intrusion activity and then based on a predefined threshold value the most prominent features related to attack are identified. These features are included in snort rule set to detect the anomalous traffic. This anomaly detection process is combined with existing signature of snort to produce the better detection. In paper [9] various types of attacks and countermeasures related to trust schemes in WSNs are categorized. The authors present the development of trust mechanisms along with short summarization of classical trust methodologies emphasizing the challenges of trust scheme in WSNs. In paper [10] a few of the key design principles relating to the development of anomaly detection techniques in WSNs are discussed in particular. The analysis and comparisons of the approaches that belong to a similar technique category are represented technically. In paper [11] Anomaly detection, one of intrusion detection system is often associated with high false alarm with moderate accuracy and detection rates when it's unable to detect all types of attacks correctly is mentioned. To overcome this problem the authors have proposed a hybrid learning approach through combination of K-Means clustering and Naïve Bayes classification. The proposed approach is to cluster all data into the corresponding group before applying a classifier for classification purpose. In paper [12] an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission is proposed. In paper [13] a Lightweight Network Intrusion Detection system (LNID) is proposed for detecting attacks which exploit code based system vulnerability on Telnet traffic. According to the performance comparisons with other network-based IDS, LNID is the most efficient on detection rate and workload reduction. In paper [14] authors have first studied intrusion detection for wireless industrial sensor networks, through various experiments and design of a hierarchical framework and then classify and select better methodologies against various intrusions. In paper [15] the authors have proposed a hybrid IDS by combining the two approaches. The hybrid IDS is obtained by combining packet header anomaly detection (PHAD) and network traffic anomaly detection (NETAD) which are anomaly-based IDSs with the misuse-based IDS Snort which is an open-source project. It is evaluated using the MIT Lincoln Laboratories network traffic data (IDEVAL). In paper [16] a specification based Intrusion Detection System for wireless sensor networks is proposed. The proposed scheme tries to optimize the local information (information collected by watch dogs) into global information (decision taken by cluster head) in order to compensate the communication pattern in network. In paper [17] a new Hybrid Intrusion Detection System (HIDS) design principles and evaluation results are reported. This hybrid system combines the advantages of low false-positive rate of signature-based intrusion detection system (IDS) and the ability of anomaly detection system (ADS) to detect novel unknown attacks.

Various authors have worked on hybrid anomaly detection but nobody has done the work on hybrid anomaly detection in WSN. But it's very important as we know security is also a serious concern in wireless sensor network.

III. PROBLEM DEFINITION

Wireless sensor networks are prone to various attacks. Sometimes multiple attacks are launched in the network degrading the performance of the network rapidly. In this situation it becomes very hard to find out which kind of anomaly is activated in the network. In this paper we have done the analysis of network data i.e. Traffic data and End to end Delay data in order to find the anomaly. The data set is clustered using Weka tool.

IV. RELATED TERMINOLOGY

In order to obtain the data set which needs to be clustered in Weka tool we have simulated the network under two different attacks i.e. Misdirection and Blackhole attack. The data set obtained from this simulation is then used to analyze and detect the anomalies in the network.

A. Misdirection Attack

In misdirection attack the attacker routes the packet from its children to other distant nodes but not necessarily to its legitimate parent. This produces long delay in packet delivery and decreases the throughput of the network. The packets reach to the destination but from a different route which further produces long delay, thus decreasing throughput of network.

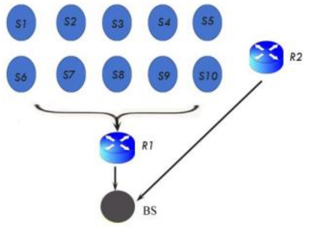


Fig. 1. Normal flow of Packets

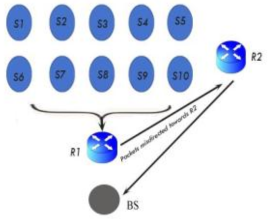


Fig. 2. Flow Packets when R1 becomes Misdirection Attacker

Figure 1 shows normal flow of packets. S1, S2, ----, S10 are sensors reporting to router R1, which further reports to coordinator (base station BS). Router R2 also reports to coordinator. Figure 2 shows the flow of packets misdirected to node R2 by the malicious node R1. Router R2 is working in collaboration with R1.

B. Blackhole Attack

Blackhole attack occurs when an intruder captures and re-programs a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station. As a result any information that enters in the black hole region is captured. Black hole attacks are easy to constitute and they are capable of undermining network effectiveness by partitioning the network such that important event information do not reach the base stations. The network performance parameters i.e. throughput and end to end delay are affected in the presence of blackhole nodes.

Blackhole attack in WSN can be performed as:

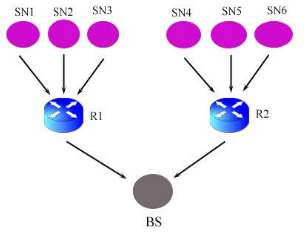


Fig. 3. Normal flow of Packets

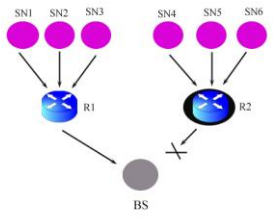


Fig. 4. Blackhole attacking scenario when router R2 becomes Attacker

1) Normal Flow of Packets:

Figure 3 shows normal flow of packets. In this scenario we have 6 sensor nodes (i.e. SN1, SN2, ----- SN6), two router nodes (R1, R2) and a base station. The sensor nodes sense any physical phenomenon, convert this into information and send this sensed and processed information to router node R1 and R2. Sensor nodes SN1, SN2 and SN3 are reporting to router R1 and SN4, SN5 and SN6 are reporting to router R2. The router R1 and R2 further sends data to the base station (BS).

2) Blackhole Attacking Scenario:

Figure 4 shows blackhole attacking scenario. In this scenario we have 6 sensor nodes (i.e. SN1, SN2, ----- SN6), two router nodes (R1, R2) and a base station. The sensor nodes sense any physical phenomenon, convert this into information and send this sensed and processed information to router node R1 and R2. Sensor nodes SN1, SN2 and SN3 are reporting to router R1 and SN4, SN5 and SN6 are reporting to router R2. The router R1 sends data to coordinator node. But router R2 becomes blackhole attacker it absorbs all the traffic coming to it and doesn't send it further to coordinator. Router R2, the blackhole node is represented by a black background here.

C. K- Means Clustering

Clustering basically is the task in which the data points are divided into homogenous classes or clusters. By homogenous it means they are similar. Items present within the same class are as much as similar. Thus this process can also be referred as Grouping.

K- Means clustering comes under the category of partitioning method in which a partition of a database *D* of *n* objects is done into a set of *k* clusters. Given a *k*, the main task is of finding a partition of *k clusters* that optimizes the chosen partitioning criterion.

The input to this algorithm is k and task is to partition a set of n objects into k clusters so that the resulting intra cluster similarity is high but the inter cluster similarity is low. Cluster similarity is measured in regards to the mean value of the object in a cluster, which can be viewed as the cluster's centroid or center of gravity.

IV. METHODOLOGY

Here we have done the analysis of dataset for multiple anomalies coexisting in the network at the same time. The data set used for detecting the anomaly existing in the network is generated in the network simulation process. The results of the simulation i.e. traffic data and end to end delay is analyzed using Weka. K-means clustering technique is used in computing the clusters from traffic and delay data. Two type of analysis is done one is using the traffic data where we find the blackhole nodes and second one is done using Delay data where we get the misdirection nodes present in the network.

The two kinds of data traffic is used i.e. traffic sent and traffic received. In traffic sent analysis we have detected Blackhole nodes. The analysis done on the traffic received helps to find the nodes working in collaboration of the misdirection attackers as they would be having high value of traffic received under attack. The nodes where high value corresponding to the delay parameter is obtained are misdirection attacker nodes. To check which node is working in collaboration with which misdirection attacker node we have to check communication range of nodes. If a node is in communication range then it can work in collaboration with that misdirection attacker node otherwise it's not possible for the node to work in collaboration.

A. Mathematical Model

For the proposed hybrid anomaly detection scheme we have developed following mathematical model.

1) Traffic Model:

a*) Traffic Sent:*

If a node is blackhole node then traffic sent under attack must be zero. Otherwise under normal flow it is having some finite value:

$Tr_{sent} = 0$, under blackhole attack
Tr_{sent} = some finite value, under normal flow

b) Traffic Received:

If a node is working correctly then it always has traffic value less than the calculated threshold.

Suppose for a node the traffic received threshold value is x, then under normal flow it is equal to or less than this value.

$Tr_{received} <= x$, under normal flow
$Tr_{received} > x$, under misdirection attack, if a node is working in collaboration with misdirection attacker node.

In this case traffic received for a node is the sum of its own traffic and traffic send by a misdirection attacker node. Suppose A is that node and B is misdirection attacker node, then traffic received will be:

$$Tr_{\text{A received}} = Tr_{\text{A received}} + Tr_{\text{B received}}$$

2) Delay Model:

In the presence of misdirection attack the delay is increased at some nodes.

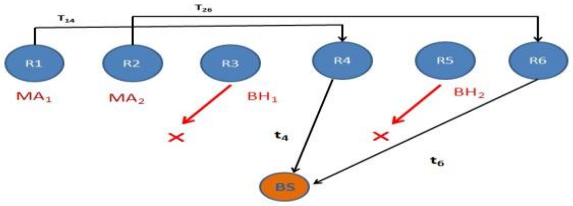


Fig. 5. Traffic flow under hybrid anomalies

Figure 5 shows traffic flow under hybrid anomalies.

For misdirection attacker nodes MA_1 and $MA_{2,}$ let us say T_1 and T_2 are delays for normal flow, if misdirection attack has occurred then in that case delay increases. T_1' and T_2' are the values of delay under attack for MA_1 and MA_2 and nodes.

$$T_1'=T_{14}+ t_4$$

T_{14} time taken by packets in reaching node R_4 from R_1, t_4 time taken by packets in reaching BS from R_4,

$$T_2'=T_{26}+ t_6$$

T_{24} is the time taken by packets in reaching R_6 from R_2, t_6 is the time taken by packets in reaching BS from R_6. So under misdirection attack:

$$T_1'> T_1$$
$$T_2'> T_2$$

V. EXPERIMENT DESIGN

A. Network Simulation Design

To generate the dataset we have simulated a wireless sensor network under normal flow and under attack. The simulation scenario consists of 18 sensor nodes.

Fig. 6. Network Scenario under normal flow

Fig. 7. Network Scenario under attack

In figure 6 we use 18 sensor nodes and build a scenario without any attacker showing a normal flow of traffic.

In figure 7 we use 18 sensor nodes and build a scenario with different attackers. R1, R2, R3 and R5 are attacker nodes.
The various design parameters are listed in table I.

1) Experiment Design Parameters:

TABLE I
COMMON PARAMETERS USED IN SIMULATION

Parameter		Value
Area		500x500 met (Fix)
Network Size	Normal Flow	18 Sensor Nodes
		06 Routers with normal flow
		01 Coordinator
	Attacking Scenario	12 Sensor Nodes
		02 Routers with normal flow
		04 Router (attacker)
		01 Coordinator
Topologies		Tree
Simulation Time		60 Minutes
Packet Inter- Arrival Time (sec)		Constant (1)
Packet Size (bits)		Constant (1024)
CSMA/CA Parameters		Default
Sensing duration (sec)		0.1

B. Results

The clustering is done using Weka and the following results are obtained:

From the dataset the following average values are obtained:

TABLE II
PERFORMANCE PARAMETERS

	End-to-end Delay (msec)		**Traffic Received (bps)**		**Traffic Sent (bps)**	
Node	**Under Attack**	**Normal Flow**	**Under Attack**	**Normal Flow**	**Under Attack**	**Normal Flow**
R1	31.01	19.09	2836.2	1868.8	1018.31	1018.31
R2	29.59	24.56	980.76	1872.21	1018.31	1018.31
R3	Infinite	13.92	1937.07	1839.22	0	1018.31
R4	9.55	20.37	3848.25	2896.78	1018.31	1018.31
R5	Infinite	10.01	1848.6	1867.66	0	1018.31
R6	19.47	14.73	3822.93	2849.56	1018.31	1018.31

TABLE III
PERFORMANCE PARAMETERS THRESHOLD VALUES

Node	End-to-end Delay (msec)	Traffic Received (bps)	Traffic Sent (bps)
R1	19.09	1868.8	1018.31
R2	24.56	1872.21	1018.31
R3	13.92	1839.22	1018.31
R4	20.37	2896.78	1018.31
R5	10.01	1867.66	1018.31
R6	14.73	2849.56	1018.31

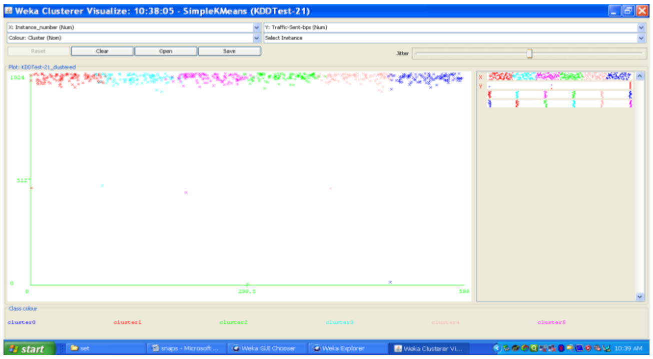
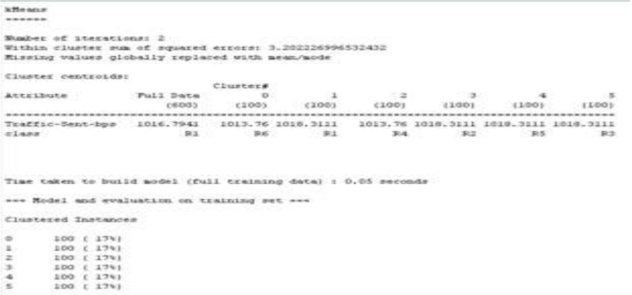


Fig. 8. Computed Clusters for Traffic sent under normal flow

Six clusters are obtained as shown in figure 8. All clusters are at the same level so this is a normal flow of traffic.



```
kMeans
======

Number of iterations: 2
Within cluster sum of squared errors: 3.2022269965324 32
Missing values globally replaced with mean/mode

Cluster centroids:
                                      Cluster#
Attribute              Full Data          0          1          2          3          4          5
                           (600)      (100)      (100)      (100)      (100)      (100)      (100)
=================================================================================================
Traffic-Sent-bps       1016.7941    1013.76 1018.3111    1013.76 1018.3111 1018.3111 1018.3111
class                         R1         R6         R1         R4         R2         R5         R3



Time taken to build model (full training data) : 0.05 seconds

=== Model and evaluation on training set ===

Clustered Instances

0       100 ( 17%)
1       100 ( 17%)
2       100 ( 17%)
3       100 ( 17%)
4       100 ( 17%)
5       100 ( 17%)
```

Fig. 9. Traffic sent by different nodes under normal flow

In figure 9 we can see that the value of traffic sent for all nodes i.e. R1, R2,---- R6 is almost same because it is normal flow of traffic.

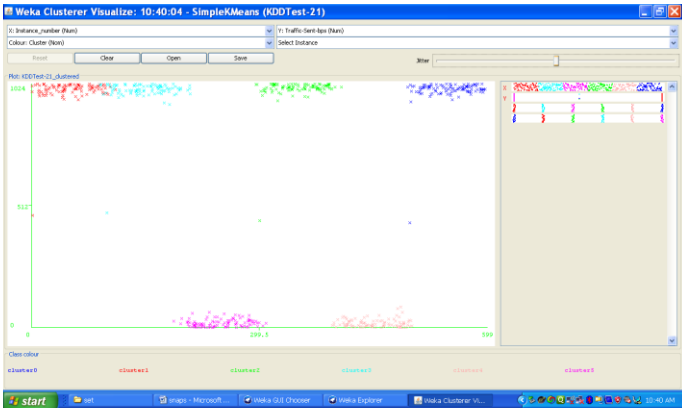
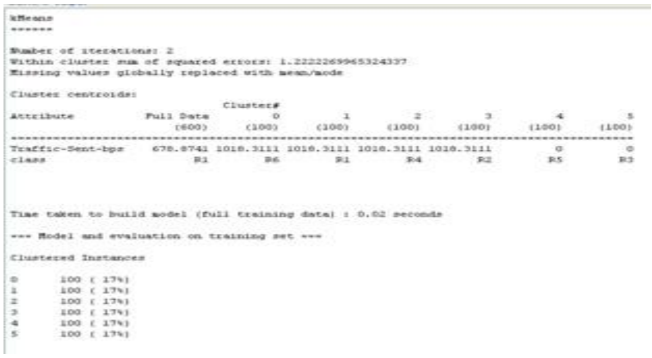


Fig. 10. Computed Clusters for Traffic sent under attack

Six clusters are obtained as shown in figure 10. Four clusters are at the same level and two clusters are at same level having almost zero value of traffic received.



```
kMeans
======

Number of iterations: 2
Within cluster sum of squared errors: 1.222226996532433 7
Missing values globally replaced with mean/mode

Cluster centroids:
                                      Cluster#
Attribute              Full Data          0          1          2          3          4          5
                           (600)      (100)      (100)      (100)      (100)      (100)      (100)
=================================================================================================
Traffic-Sent-bps        678.8741 1018.3111 1018.3111 1018.3111 1018.3111          0          0
class                         R1         R6         R1         R4         R2         R5         R3



Time taken to build model (full training data) : 0.02 seconds

=== Model and evaluation on training set ===

Clustered Instances

0       100 ( 17%)
1       100 ( 17%)
2       100 ( 17%)
3       100 ( 17%)
4       100 ( 17%)
5       100 ( 17%)
```

Fig. 11. Traffic sent by different nodes under attack

In figure 11 the value of the traffic sent by R3 and R5 is 0 bps as compared to the threshold value of R3 and R5 which is 1018.31 bps (Refer Table III). Thus nodes R3 and R5 are detected to be blackhole nodes.

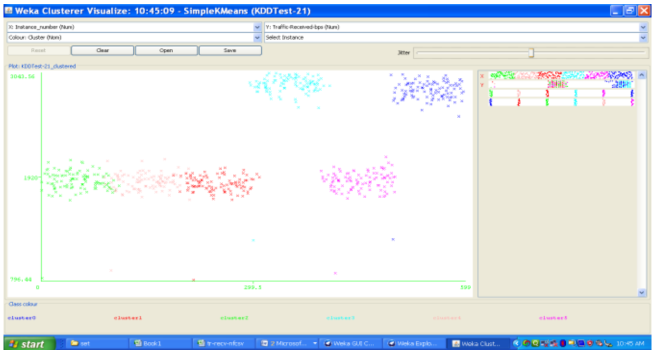
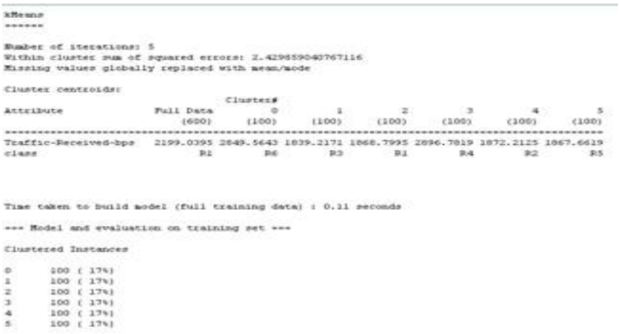


Fig. 12. Computed Clusters for Traffic received under normal flow

Six different clusters are formed as shown in figure 12; two of them are having higher value of traffic received.



```
kMeans
======

Number of iterations: 5
Within cluster sum of squared errors: 2.429859040767116
Missing values globally replaced with mean/mode

Cluster centroids:
                                     Cluster#
Attribute               Full Data          0          1          2          3          4          5
                            (600)      (100)      (100)      (100)      (100)      (100)      (100)
====================================================================================================
Traffic-Received-bps    2199.0395  2849.5643  1839.2171  1868.7995  2896.7819  1872.2125  1867.6619
class                          R1         R6         R3         R1         R4         R2         R5



Time taken to build model (full training data) : 0.11 seconds

=== Model and evaluation on training set ===

Clustered Instances

0       100 ( 17%)
1       100 ( 17%)
2       100 ( 17%)
3       100 ( 17%)
4       100 ( 17%)
5       100 ( 17%)
```

Fig. 13. Traffic received at different nodes under normal flow

We have seen that six different clusters are formed two of them are having higher value of traffic received. The clusters of R1 and R6 are having higher values but it matches with the threshold values so there is not any attacker in the network.

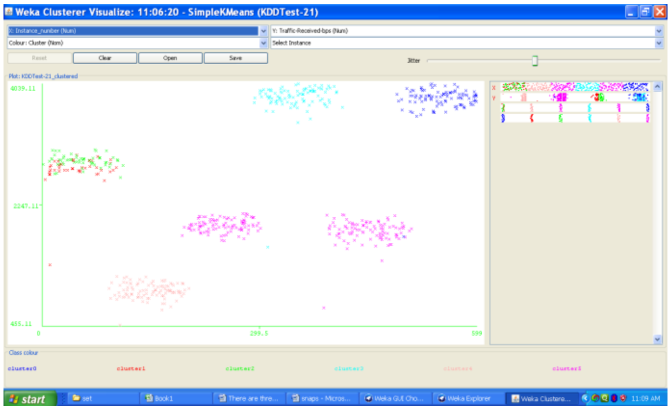
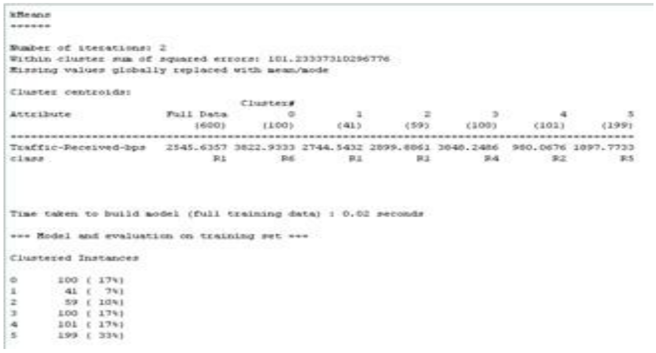


Fig. 14. Computed Clusters for Traffic received under attack

Six different clusters are formed as shown in figure 14; two of them are having higher values of traffic received.



```
kMeans
======

Number of iterations: 2
Within cluster sum of squared errors: 101.23337310296776
Missing values globally replaced with mean/mode

Cluster centroids:
                                     Cluster#
Attribute               Full Data          0          1          2          3          4          5
                            (600)      (100)       (41)       (59)      (100)      (101)      (199)
====================================================================================================
Traffic-Received-bps    2545.6357  3822.9333  2744.5432  2899.8861  3848.2486   980.0676  1097.7733
class                          R1         R6         R1         R3         R4         R2         R5



Time taken to build model (full training data) : 0.02 seconds

=== Model and evaluation on training set ===

Clustered Instances

0       100 ( 17%)
1        41 (  7%)
2        59 ( 10%)
3       100 ( 17%)
4       101 ( 17%)
5       199 ( 33%)
```

Fig. 15. Traffic received at different nodes under attack

We have seen that six different clusters are formed two of them are having higher value of traffic received. The clusters R4 and R6 traffic received values are 3848.25 bps and 3822.93 bps respectively which are very high as compared to the threshold values i.e. 2896.78 and 2849.56 respectively (Refer Table II and III). Thus R4 and R6 are detected as the nodes working in collaboration with misdirection attacker nodes.

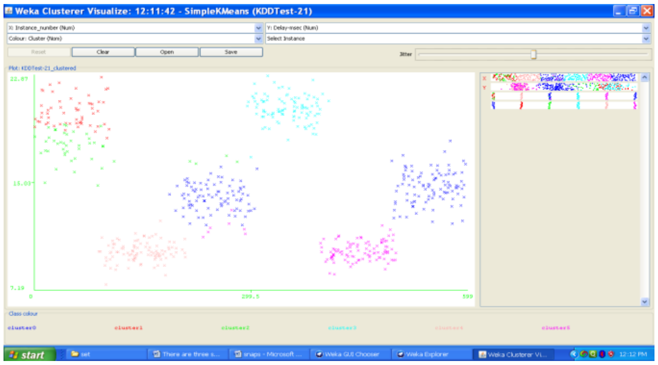
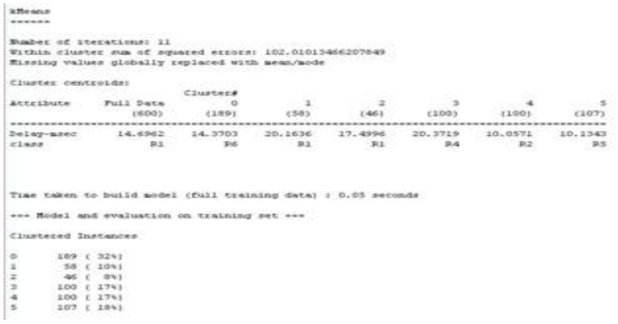


Fig. 16. Computed Clusters for Traffic received under normal flow

Six different clusters are formed as shown in figure 16; two of them are having higher value.



```
kMeans
======

Number of iterations: 11
Within cluster sum of squared errors: 102.01013466207849
Missing values globally replaced with mean/mode

Cluster centroids:
                           Cluster#
Attribute     Full Data          0          1          2          3          4          5
                  (600)      (189)       (58)       (46)      (100)      (100)      (107)
==========================================================================================
Delay-msec      14.6962    14.3703    20.1636    17.4996    20.3719    10.0571    10.1343
class                R1         R6         R3         R1         R4         R2         R5



Time taken to build model (full training data) : 0.05 seconds

=== Model and evaluation on training set ===

Clustered Instances

0       189 ( 32%)
1        58 ( 10%)
2        46 (  8%)
3       100 ( 17%)
4       100 ( 17%)
5       107 ( 18%)
```

Fig. 17. End-to-end Delay of different nodes under normal flow

We have seen that six different clusters are formed two of them are having higher value of end to end delay. The clusters of R1 and R4 are having higher values but it matches with the threshold values so there is no attacker in the network.

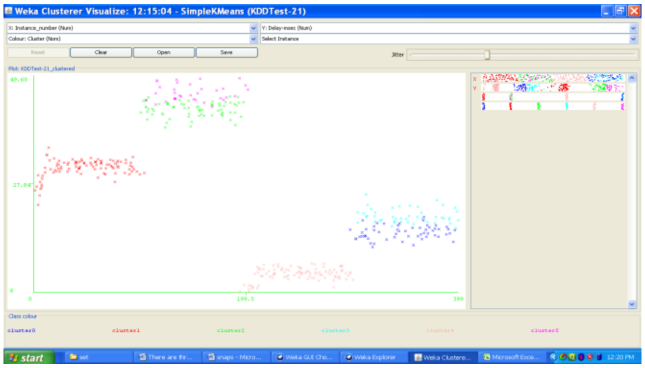
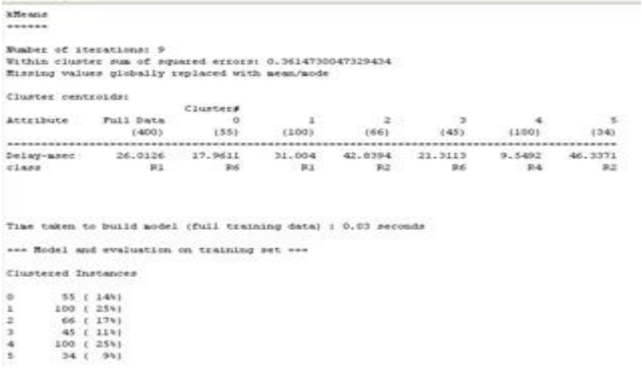


Fig. 18. Computed Clusters for Traffic received under attack

Six different clusters are formed as shown in figure 18; two of them are having higher value of traffic received.



```
kMeans
======

Number of iterations: 9
Within cluster sum of squared errors: 0.3614730047329434
Missing values globally replaced with mean/mode

Cluster centroids:
                         Cluster#
Attribute     Full Data         0          1          2          3          4          5
                  (400)      (55)      (100)       (66)       (45)      (100)       (34)
==========================================================================================
Delay-msec      26.0126   17.9611     31.004    42.8394    21.3113     9.5492    46.3371
class                R1        R6         R1         R2         R6         R4         R2




Time taken to build model (full training data) : 0.03 seconds

=== Model and evaluation on training set ===

Clustered Instances

0        55 ( 14%)
1       100 ( 25%)
2        66 ( 17%)
3        45 ( 11%)
4       100 ( 25%)
5        34 (  9%)
```

Fig. 19. End-to-end Delay of different nodes under attack

We have seen that six different clusters are formed two of them are having higher values for end to end delay. The threshold values of R1 and R2 for end to end delay are 19.09 ms and 24.56 ms respectively as compared to the values obtained of 31.01ms and 29.59 ms respectively (Refer Table II and III). Thus R1 and R2 are detected as misdirection attacker nodes. Since R4 is nearer to R1 and R6 is nearer to R2 so R4 is working with R1 and R6 is working with R2.

VI. KEY FINDINGS

The sensor network is simulated, dataset is generated then this data set is analyzed using Weka and clusters are formed. During the analysis the following observations were made:

- Router R1 and R2 are misdirection attackers and Router R4 and R6 are working in collaboration with these nodes. R1 misdirects traffic to R4 and R2 to R6 (Refer figure 18 and 14).
- Router R3 and R5 are blackhole attacker nodes (Refer figure 10).

VII. CONCLUSION

The clustering is done using Weka tool by K-means clustering technique. The proposed model is capable of detecting the hybrid kind of anomalies existing in a sensor network. The described method is capable of finding the blackhole nodes and misdirection nodes just by analysis two types of network parameters i.e. traffic data and end to end delay data. Blackhole nodes are the ones which don't forward the traffic and absorb all the packets reaching them. Thus their detection is done by comparing the traffic sent values which are generally zero for them. Misdirection nodes misdirect the traffic thus increasing the delay values sometime making it infinite also. Thus these nodes are detected using end to end delay parameter values.

This work can be extended further by adding more anomalies like Sink Hole, Gray Hole etc. in the network.

REFERENCES

[1] Reda M. Elbasiony, Elsayed A. Sallam, Tarek E. Eltobely, Mahmoud M. Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means", Elsevier Journal of Ain Shams Engineering, 2013.

[2] Roshan Singh Sachan, Mohammad Wazid, D P Singh, Avita Katal, R H Goudar, "Misdirection Attack in WSN: Topological Analysis and an Algorithm for Delay and Throughput Prediction", Proceedings of 7th International Conference on Intelligent Systems and Control (ISCO'13) 2013.

[3] Basant Agarwal, Namita Mittal, "Hybrid Approach for Detection of Anomaly Network Traffic using Data Mining Techniques", Elsevier Journal of Procedia Technology, Volume 6, 2012, Pages 996–1003.

[4] K. Qazanfari, M.S. Mirpouryan, H. Gharaee, "Novel hybrid anomaly based intrusion detection method", IEEE Sixth International Symposium on Telecommunications (IST), 2012.

[5] Roshan Chitrakar, Chuanhe Huang, "Anomaly Based Intrusion Detection Using Hybrid Learning Approach of Combining k-Medoids Clustering and Naïve Bayes Classification", IEEE 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2012.

[6] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", IEEE Transactions on Network and Service Management, (Volume:9, Issue: 2), June 2012.

[7] A.S Aneetha , T.S. Indhu, S. Bose, "Hybrid network intrusion detection system using expert rule based approach", ACM, Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology (CCSEIT), 2012.

[8] K.V.Arya, Hemant Kumar, "A clustering based algorithm for network intrusion detection" ACM, Proceedings of the Fifth International Conference on Security of Information and Networks, 2012.

[9] Yan Li Yu, Keqiu Li, Wanl Zhou, Ping Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", Elsevier, Journal Of Network Computer and Applications, Special Issue on Trusted Computing and Communications, May 2012 Volume 35, Issue 3, Pages 867–880.

[10] Miao Xie, Song Han, Biming Tian, Sazia Parvin, "Anomaly detection in wireless sensor networks: A survey", Elsevier Journal of Network and Computer Applications, Volume 34, Issue 4, July 2011, Pages 1302–1325.

[11] Z. Muda, W.Yassin, M. N Sulaiman, N. I Udzir, "Intrusion detection based on K-Means clustering and Naïve Bayes classification", IEEE 7th International Conference on Information Technology in Asia, 2011.

[12] Satyajayant Misra, Kabi Bhattarai, Guoliang Xue, "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks", IEEE International Conference on Communications (ICC) 2011.

[13] Chia-Mei Chen, Ya-Lin Chen, Hsiao-Chung Lin, "An efficient network intrusion detection", Elsevier Journal of Computer Communications, Volume 33, Issue 4, 1 March 2010, Pages 477–484.

[14] Sooyeon Shin , Taekyoung Kwon ,Gil-Yong Jo , Youngman Park, "An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks", IEEE Transactions on Industrial Informatics, (Volume:6 , Issue: 4), Nov. 2010.

[15] M. Ali Aydın, A. Halim Zaim , K. Gökhan Ceylan, "A hybrid intrusion detection system design for computer network security", Elsevier Journal of Computers & Electrical Engineering, Volume 35, Issue 3, May 2009, Pages 517–526.

[16] Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari, Kumar Sidharth Choudhary, "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information", IEEE 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT) 2009.

[17] Kai Hwang, Min Cai, Ying Chen, Min Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes", IEEE Transactions on Dependable and Secure Computing (Volume:4 , Issue: 1) , 2007.