Bayesian Correlated Equilibrium Based IDS for MANET

S. Sampath\textsuperscript{1} and A. Edwin Robert\textsuperscript{2}

\textsuperscript{1}Department of Computer Science, Karpagam University, Coimbatore - 641021, Tamil Nadu, India; sampathphd2016@gmail.com
\textsuperscript{2}Department of Computer Applications, Karpagam University, Coimbatore - 641021, Tamil Nadu, India; edrt.edwin@gmail.com

\textbf{Abstract}

\textbf{Objective}: To improve IDS strategy with high detection accuracy and reduce the power consumption of the nodes in MANET. \textbf{Methods}: There are several intrusion detection systems are developed. In order to increase the performance of IDS, Bayesian Correlated Equilibrium based IDS which incorporates two main processes namely, Cluster Head selection and Hybrid IDS for MANET is proposed. The game theory is also used to increase the detection accuracy of IDS. \textbf{Findings}: Mobile Ad-hoc Network (MANET) is an autonomous system that consists of battery powered mobile nodes. MANETs are prone to several attacks as they are continuously self configuring and infrastructure less. As the nodes are mobile, they are susceptible to intrusions. The Intrusion Detection System has issues of heavy traffic related to IDS in the network, which causes congestion. It also leads to high energy consumption among the nodes. So designing an efficient MANET should have certain number of goals such as effective intrusion detection, light traffic and low energy consumption and power loss. Many Intrusion detection schemes were proposed that normally incurs power loss in the node as there is a need for continuous monitoring. \textbf{Application/Improvements}: To increase detection accuracy, decrease power consumption and the IDS traffic Bayesian Correlated Equilibrium based IDS for MANET is presented.

\textbf{Keywords}: Bayesian Nash Equilibrium, Correlated Equilibrium, Game Theory, Intrusion Detection System (IDS), Mobile Ad-hoc Network (MANET)

1. Introduction

MANETs are used in a wide range of critical applications as it has a prominent technology. However, the dynamic and volatile nature of the MANET make less robust to attacks or intrusions. Several Intrusion Detection Systems were developed to monitor the system activities and give the reports to the base station. Intrusion Detection System (IDS) in MANET detects the malicious nodes that can start attacks against other normal nodes and weaken the overall performance of the entire network.

In MANETs, IDS is practiced on each node in the network to offer a centralized monitoring in MANETs. If IDS is practiced in every node in the network the battery life will be affected. Recently most of all MANET IDS system does not take into consideration of the environment they are operating in and it directs to end up monitoring all nodes with similar probability, unparticular of whether or not the node being examined has a history profile of being malicious. This reduces the examining strategy wherein the node operating the IDS turns out to be reducing most of its energy monitoring the normal nodes. The Intrusion Detection System also has issues of heavy traffic related to IDS in the network, which causes congestion. It also leads to high energy consumption among the nodes. So designing an efficient MANET should have certain number of goals such as effective intrusion detection, light traffic and low energy consumption and power loss.

Thus game theory concept was included in the IDS when there is a non competitive game conducting between the two competing players. In this game the attacker is...
considered as malicious node and the defender player is considered as the cluster head. Thus in this game the aim of defender is to improve its probability of successful intrusion detection on the other hand the aim of attacker is to reduce its probability of being detected by the IDS. Game theory makes decisions based on the type of the node being monitored by assessing the history profile of its actions.

In proposed clustering and data mining techniques for detecting the occurrence of intrusion. In the proposed clustering method utilized an efficient clustering technique called fixed width algorithm. Thus DOS attacks and sink hole attacks at various layers of protocol stack was determined by fixed width algorithm. Then the association process is carried in the proposed technique through fast apriori algorithm. With the help of fast apriori algorithm the speed of intrusion detection is increased in the network. Thus the computation speed of intrusion detection is better than the traditional techniques. The different types of UDP flooding attack was detected effectively than the proposed clustering technique.

In proposed an effective architecture for intrusion detection. The proposed intrusion detection architecture was built based on clusters, quantitative and agents which is apt for multi-hop mobile ad hoc networks. This architecture effectively determines abnormalities and nodes misbehavior such as delaying of nodes, modifying and dropping because of intermediate nodes. The efficiency of IDS architecture was evaluated using false positive rate and it proves it reduced the false positive rate for intrusion detection. However, it is suitable only for routing layers.

In proposed a new model with the mixture of SVM classification methods, outlier detection and attribute selection for Mobile Ad-hoc Network called agent-based intrusion detection model. In this model the detection accuracy was increased and the processing time was reduced using a preprocessing technique. The intruders were detected by proposed an Intelligent Agent-based Enhanced Multiclass Support Vector Machine algorithm and Intelligent Agent Weighted Distance Outlier Detection algorithm and in a distributed database environment. These two algorithms utilized intelligent agents for that use intelligent agents for transaction processing coordination and trust management.

In proposed a cooperative and distributed architecture for detection of intruders in a network. Thus the proposed architecture removed the flaws and weakness involved in existing MANET Intrusion Detection Systems (IDSs) by combining various agent based detection process. The main contribution of the proposed work depends on the distribution of network was attained through the execution of local Intrusion Detection System on each and every network node and one more contribution is the cooperation is promised by collaboration of stationary and mobile agents in a network. By this contribution IDS was achieve fault tolerance, flexibility, reactivity, distribution and co operation, lightweight and autonomy which are plays an significant role in the MANET Intrusion Detection System.

In introduced a novel collaborative-based WIDPS architecture. In this paper, MCI technique is analyzed in terms of false alarm rate and enhancing the efficiency of detection. It is clearly shown that cooperative learning-based detection that satisfied the requirements of WIDPS was described in the proposed system. This paper presents the state-of-the-art in the field of WIDPS and highlights the central problems to be tackled. However it has low detection efficiency as it does not support for multi-dimensional data.

In proposed a generalized intrusion detection and prevention mechanism for security purpose of MANET by detecting intruders in a network. This proposed work is a combination of knowledge based and anomaly based intrusion detection. In this proposed work it can able to determine new unexpected attacks like with an affordable network overhead, multiple concurrent different attacks and determine and separate the intruders causing different types of attacks. The proposed approach on the MANET performance with types of intrusion response and different attacks was tested to show its efficiency. However there is a necessary for an adaptive intrusion response in the network.

In introduced adaptive response and intrusion detection for MANETs. In this proposed work detects a range of attacks and also gives a significant response at low network deprivation. The insufficiencies of fixed response to an intrusion were analyzed. Then flexible response scheme was introduced to overcome these insufficiencies. This proposed scheme based on the degradation in network performance, measured confidence in the attack and the severity of attack. However, it incorporates higher false positives.

In an architectural model of a MANET was developed and based on the developed architectural model the
communication between the mobile was created. At the point of network congestion or due to selfish node MANET can have the packet drops. This creates an issue during communication between mobiles. Such issues will be overcome by using proposed Record- and Trust-Based Detection (RTBD) technique that is used to detect the selfish nodes. The proposed method accelerates the detection of misbehaving nodes and on necessary network functions such as packet dropping and routing.

In proposed a lightweight, energy-efficient system that works with the mobile agents through energy utilization of the sensor nodes as a metric for intrusion detection. The energy utilization of the sensor nodes were predicted by linear regression model. Simulation results demonstrates that denial-of-service attacks indicate that denial-of-service attacks, such as flooding can be detected with high accuracy, while keeping the number of false-positives very low.

In studied different architectures of IDS for MANETs and also analyzed their strengths and weaknesses. Then a new IDS architecture for MANET is proposed which is a combination of hierarchical model based on clusters and cooperation model based on a Multi-Agent System (SMA). The proposed method suits for detection decision since it was not centralized to the node as the Cluster Head in the architecture. Different nodes of group in the network make decision through actuators agents when malicious activity is detected. This method reducing attacks in the network and also the designated node consumes less energy because it shares information with different nodes of the group.

In proposed a distributed self adaptive Intrusion Detection System (IDS) that was based on programmable mobile agents. These mobile agents act as a key line of defense against major security attacks. Proposed intrusion detection model was a combination of the two trends namely the rule based and the behavior based scheme and it also includes the merits of both the host based and networks based IDSs. The proposed work considered the critical features of MANETs that is conscious of the inherent constraints of MANETS and is self adaptive. As the proposed work used light weight mobile agents a low overhead mechanism was introduced that suits characteristics of the MANET.

In proposed a new class of stealth network attacks known as mobility-based evasion. An innovative solution that leverages a novel way for NIDS cooperation was proposed. In the proposed scheme shared internal state information among multiple NIDSs deployed in different networks or network segments. The solution is integrated into a prototype which extends Snort and it is based on a lightweight agent and a set of plug ins handling different protocols. The proposed design guaranteed flexibility in terms of deployment and expandability. However, route optimization can be activated only if the correspondent node supports it.

The Intrusion Detection System needs continuous monitoring that may lead to power depletion in nodes. In order to solve this problem a Bayesian game formulation was presented earlier that had an IDS scheme formed by Vickrey-Clarke–Groves’s mechanism Cluster Head selection and a hybrid IDS of light weight and heavy weight module. The system initially activates light weight module and then the decision of activating heavy weight module is achieved by modeling ID process as a game between leader and malicious node. This system reduced the IDS traffic and power consumption and increased the detection rate and accuracy. However, the false positive rate is high for both light weight and heavy weight modules and also detection accuracy has to be increased. In order to solve all these problems, this paper proposes IDS for MANET that is clearly explained in the following sections.

2. Bayesian Correlated Equilibrium based IDS for MANET

This paper proposes Bayesian Correlated equilibrium based IDS for MANET with objectives such as improved detection of intrusion in the network by formulating in as Bayesian game with correlated equilibrium, minimizing the power consumption and intrusion related traffic in the network and also to develop IDS with high detection rate and accuracy.

The proposed system has two main process namely Cluster Head election process and a hybrid IDS for detection. This hybrid IDS consists of light weight and heavy weight models. The lightweight module is less powerful and uses simple analytical rules based on threshold values to detect intrusions. But, the heavyweight module is more powerful and uses complex association-mining rule techniques to detect anomalies. Initially the
MANET is divided into clusters with the help of standard clustering algorithm in 15. Each node in the cluster should be in the transmission range of the cluster. The nodes possess the parameters such as maliciousness value $m_i$, reputation value $r_i$ and energy value $e_i$. The cluster nodes elect the Cluster Head using VCG algorithm. These Cluster Head performs intrusion detection in all the other cluster nodes for a specific period of time as it can be replaced by other efficient nodes later. The Cluster Head node may misbehave by not detecting the intrusion and present that malicious node to be normal. In such cases, checker nodes watch the Cluster Head and if it misbehaves, a punishment of lowering its reputation value is provided such that a new Cluster Head will be elected.

After the election, the Cluster Head assigns the $m_i$ value to all the cluster nodes $N_i$. Then light weight module is activated to monitor the nodes to determine it is an attacker or normal node. It checks the PFR ratio of the each node which is described as the ratio of total number of packets received to the total number of packets forwarded over a given interval of time. From the value of PFR we can easily identify the attacker by if PFR is less than a threshold, then the node is an attacker, else it is legitimate user. If the node is an attacker, the offensiveness value is updated and then the heavy weight module is activated. Otherwise if the node is a legitimate user, the $m_i$ value is updated however the activation of heavy weight module is identified with the help of interaction of malicious node and Cluster Head. The Bayesian Correlated Equilibrium

**Figure 1.** Overall flow of the proposed methodology.
(BCE) of the game model has equivalent mixture of the strategy which concludes the activation of the heavy weight model. The heavyweight module is an anomaly based IDS in which the association-rule mining technique to identify the action of $N_i$ as attack or normal. If the action of $N_i$ is known to be normal by the heavyweight module then the $m_i$ value of $N_i$ is reset to $N_i/2$; otherwise, the $m_i$ value of $N_i$ is retained. The Figure 1 shows overall flow of proposed methodology.

2.1 Cluster Head Election by VCG Technique

MANET nodes are clustered efficiently and the each node in the cluster should be in the transmission range of the cluster. The cluster nodes elect the Cluster Head using VCG algorithm. These Cluster Head performs intrusion detection in all the other cluster nodes for a specific period of time as it can be replaced by other efficient nodes later. Re-election is conducted to elect a new leader node after the timer expires. Random node can be elected as a Cluster Head without considering the energy level of the nodes which may cause faster death of the nodes with low energy level. Therefore the election mechanism should consider some selfish nodes that are unwilling to participate in the election as they have higher energy levels not to be wasted. A reputation based leader node election is utilized where nodes with higher reputations are considered as more trusted nodes and are given priority to be elected as Cluster Head.

2.2 Hybrid IDS for MANET

The defender player should continuously monitor the attacker player continuously at every game stage to update the node's belief which is quiet energy consuming. In order to minimize the energy consumption, a two layered hybrid IDS detection model is used. The hybrid IDS has two modules, light weight and heavy weight module. The light weight module is less powerful but requires lesser energy for its operation where as the heavy weight module is powerful and needs more energy to be consumed. Initially the light weight module is activated and then on a need to take rigorous analysis of the malicious node, the heavy weight module is activated.

2.2.1 Heavy Weight Intrusion Detection System (HIDS)

The HIDS uses associative rule mining technique on transmission events to detect the associative patterns and then build rules to define the normal profile of the network using Apriori Algorithm. The features that are extracted from the Mac and network layer are Packet event type, Sender address, Destination Address, MAC frame type, Route control packet type, Route change percentage.

2.2.2 Light Weight Intrusion Detection System (LIDS)

Heavy weight module consumes more energy, hence an alternative light weight monitoring system is used to update the malicious belief values of the nodes for every stages of the game. The LIDS being a light weight module uses simple rules and methods to detect intrusions. The value of Packer forwarding rate of each node is checked and if any node's value goes below a pre defined threshold, the node is assumed to be malicious and its belief value is updated using Bayes rule. If the Cluster Head and the attacker game being extensive then the correlated equilibrium is used to obtain the probability of the heavy weight IDS module.

3. Bayesian Game model for IDS

The game theory provides stable outcome in situations when two or more decision makers with different intentions compete for a same resource. The interaction between the monitoring node and the potential malicious node in a MANET are the two players in the static Bayesian game. The player $P_i$ is a potential attacker and the other player $P_j$ is a defender. The private information of the attacker node is based on the value $v_i$. If $v_i$ is 0 then the node is normal and if $v_i$ is 1 then it is malicious. The attacker player has two strategies

For $v_i = 0; \{\text{Attack, Not attack}\}$, for $v_i = 1; \{\text{Not Attack}\}$.

Similarly, for defender player one strategy $v_j = 1; \{\text{Monitor, Not Monitor}\}$.

The strategies are chosen by the players at the beginning of the game considering about the costs effectiveness in monitoring and attacking any given node in the network. This non cooperative incomplete information game between the two players $P_i$ and $P_j$ can be represented as a triplet.

$G = \{N, S, U\}$, where $N = \{P_i, P_j\}$ the players of the game, $S = S_i \times S_j$ is the strategy space of the game with $S_i$ and $S_j$ are individual strategy space of the players, $U = U_i \times U_j$ is the pay off utility corresponding to the
strategy space S of the game. Ui and Uj are for the players respectively. C is the cluster f nodes with C = \{n1, n2, n3 … nk\}. Consider any node nk in the in the cluster, with asset value wk.

The payoff values corresponding to the interaction between the attacker and the defender is calculated on the basis of the reputation value of the node nk, cost involved in the attack C\_ak, monitoring cost C\_mk, detection rate, false alarm rate (α) etc. Table 1 explains the pay off values when the type of attacker player is malicious and table 2 when the player is normal.

Table 1. Payoff matrix when the player is malicious

| Attack       | Monitor | Not Monitor |
|--------------|---------|-------------|
| Attack       | (1-2α)wk - C\_ak, (2α - 1) wk - C\_mk | wk – C\_ak, - wk |
| Not Attack   | 0, - γ wk - C\_mk | 0, 0 |

Table 2. Payoff matrix when player is normal

| Not Attack | Monitor | Not Monitor |
|------------|---------|-------------|
| Not Attack | 0, - γ wk - C\_mk | 0, 0 |

3.1 Bayesian Correlated Equilibrium

The game between the defender and the attacker is extensive in case the defender player is unaware about the type of the player whether is normal or malicious and the action whether it decides to attack or not attack. Thus it is assumed that the both the players have a goal to maximize their respective payoffs. That is for defender it should increase the probability of detecting the malicious node and for the attacker should decrease the probability of getting detected.

A correlated equilibrium determines an effective solution when there is an extensive game in the network between the two players. Thus this equilibrium is a correlated strategy for the players implemented by a mediator that makes non binding recommendations to each player. Assume that there is a mediator that recommends a particular strategy to players. Based on the recommendation, the player can choose it or opt other strategy from its set.

3.2 Correlated Equilibrium

• Assume that each player learns only the strategy recommended to that player by the mediator.

• Suppose the mediator recommends an attack strategy for the player I, then the player knows that defender is recommended for Not Monitor. Thus when the defender does not monitor, it is the best response for the attacker to attack. So the attacker would be happy to attack by accepting the recommendation of the mediator.

• Suppose the mediator recommends not attack for the player i, knowing that the mediator might have recommended the mixed strategy of monitor and non monitor for the defender. When the defender monitors or not monitors, the attacker gets a payoff even if it attacks or not attack.

• Thus the attacker never minds the mediator recommendation.

From this sequence, it is clear that attacker listens to the mediator if and only if the defender listens to the mediator. Similarly defender chooses the mediator’s options under the belief that attacker obeys the mediator. This shows that the two players can reach a self-enforcing understanding to obey the mediator if the mediator recommends the correlated strategy.

Let K belongs to the ∆(S) be the correlated strategy recommended by the mediator. And K is the knowledge. The Strategy K induce an equilibrium for the two players to obey the mediator if:

\[
\sum_{i \in S} K_i(S_i) \leq K(S) \geq \sum_{i \in S} K_i(S_i) - U_i(S_i)
\]

(1)

Where \[U_i(S_i)\] is the strategy that player i obeys the mediator. Such a strategy K is called a correlated equilibrium.

\[
\sum_{i \in S} K_i(S_i) \leq K(S) \geq \sum_{i \in S} K_i(S_i) - U_i(S_i)
\]

(2)

Equation 2 shows the strategy when player I disobeys mediator and also to expect a payoff. It is to be noted that K(S)≥ 0 for all values of S. Such that:

\[
\sum_{i \in S} K_i(S_i) - 1
\]

(3)

It can be shown that the set of all correlated equilibria in a finite game is a compact and convex set.

The feasible solution is obtained by solving the linear problem,

\[
\max \sum_{i \in S} K_i(S_i)
\]

(4)
That subjects to 
\[
\sum_{s'} R(S_1, S_2, s')(U(S_1, S_2) - U(S_2')) \geq 0
\]
and 
\[
\sum_{s'} R(s') = 1.
\]

An optimal solution of this linear program will give a correlated equilibrium that maximizes the intrusion detection of the IDS.

Thus this equilibrium state determines the probability value to activate the heavy weight module to analyze the malicious node and reduce its reputation value if it is an attacker and reins the same if it is normal.

4. Experimental Results

The proposed Bayesian Correlated Equilibrium Based IDS for MANET is tested for its effectiveness using the parameters such as Packet Delivery Ratio, Detection Rate, Throughput and Delay. These parameters are evaluated and compared with the existing Bayesian game model - Hybrid IDS technique to prove that the proposed scheme outstands from all other existing IDS techniques.

4.1 Packet Delivery Ratio

Packet Delivery Ratio (PDR) refers to the ratio of the number of packets delivered to the destination node against the number of packets generated by the source node.

4.2 Detection Rate

The Detection Rate is defined as the number of intrusion instances detected by the system (True Positive) divided by the total number of intrusion instances present in the test set.

4.3 Network Throughput

Network throughput is the rate of successful message delivery over a communication channel.

4.4 Detection Delay

Detection Delay is the time delay in detecting the mobile intruder in the network by the defender or the IDS itself.

Figure 2 shows the Packet Delivery Ratio (PDR) comparison of the Bayesian game model-Hybrid IDS and the proposed Bayesian Correlated Equilibrium based IDS for MANET. The PDR value of the two schemes is evaluated for increasing number of nodes in the network. The comparison result show that the proposed method stands out in high Packet Delivery Ratio.

Figure 3 shows the Detection Rate Comparison of the Bayesian game model-Hybrid IDS and the proposed Bayesian Correlated Equilibrium based IDS for MANET. The detection rate value of the two schemes is evaluated for increasing number of malicious nodes in the network. The comparison result shows that the proposed method has the improved detection rate than Hybrid IDS.

Figure 4 shows the Network Throughput Comparison of the Bayesian game model-Hybrid IDS and the proposed Bayesian Correlated Equilibrium based IDS for MANET. The throughput value of the two schemes is evaluated for increasing number of malicious nodes in the network. The comparison result shows that the proposed method have high network throughput compared to the Hybrid IDS.

Figure 5 shows the Network Delay Comparison of the Bayesian game model - Hybrid IDS and the proposed Bayesian Correlated Equilibrium based IDS for MANET. The Delay value of the two schemes is evaluated for increasing number of nodes in the network. The comparison result shows that the proposed method proves to be faster in detecting the malicious nodes in the network.

Figure 2. Packet Delivery Ratio comparison.
Cluster Head election and Hybrid IDS which incorporated Bayesian Correlated Equilibrium. Initially the clustered MANET elects Cluster Head for each cluster using VCG technique. Then Hybrid IDS model is initialized in the Cluster Head to detect intrusions in the network. First the light weight IDS is activated to detect the malicious node. A Bayesian game is used to model the interaction between the Cluster Head and the malicious node. As the malicious node can resist from being detected, there is an extension in the game, where the detection of attacker is handed over to the heavy weight module which is activated on the basis of the correlated equilibrium technique. The correlated equilibrium technique is used to lower the risk of high computational cost caused by earlier methods. It only requires solving a linear problem assuming that no player wants to deviate from the recommendation of the mediator strategy assuming the opponent will not deviate. Thus an efficient IDS strategy with high detection accuracy is designed to reduce the IDS traffic and also the power consumption of the nodes.

6. References

1. Devi VA, Bhuvaneswaran RS. Agent based cross layer Intrusion Detection System for MANET. Advances in Network Security and Applications. Springer Berlin Heidelberg; 2011. p. 427–40.
2. Karami M, et al. QAIDS: Quantitative and agent based Intrusion Detection System. Computer and Information Science. 2011; 4(2); (2011):64–74.
3. Ganapathy S, Yogesh P, Kannan A. Intelligent agent-based Intrusion Detection System using enhanced multiclass SVM. Computational Intelligence and Neuroscience. 2012; (2012):9.
4. Mechtri L, Tolba FD, Ghanemi S. MASID: Multi-Agent System for Intrusion Detection in MANET. 2012 IEEE Ninth International Conference on Information Technology: New Generations (ITNG); 2012.
5. Shamshirband S, et al. An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. Engineering Applications of Artificial Intelligence. 2013; 26(9):2105–27.
6. Nadeem A, Howarth M. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. Telecommunication Systems. 2013; 52(4):2047–58.
7. Nadeem A, Howarth MP. An intrusion detection and adaptive response mechanism for MANETs. Ad Hoc Networks. 2014; 13:368–80.
8. Subramaniyan S, Johnson W, Subramaniyan K. A distributed framework for detecting selfish nodes in MANET.
using Record-and Trust-Based Detection (RTBD) technique. EURASIP Journal on Wireless Communications and Networking. 2014; 2014:1–10.

9. Riecker M, et al. Lightweight energy consumption-based Intrusion Detection System for Wireless Sensor Networks. International Journal of Information Security. 2015; 14(2):155–67.

10. Chadli S, et al. A new model of IDS architecture based on multi-agent systems for MANET. IEEE 2014 Second World Conference on Complex Systems (WCCS); 2014.

11. Krishnan D. A distributed self-adaptive Intrusion Detection System for Mobile Ad-hoc Networks using tamper evident mobile agents. Procedia Computer Science, 2015; 46:1203–8.

12. Amudhavel J, Brindha V, Anantharaj B, Karthikeyan P, Bhuvaneswari B, Vasanthi M, Vinodha D. A survey on Intrusion Detection System: State of the Art Review. Indian Journal of Science and Technology, 2016; 9(11).

13. Andreolini M, Colajanni M, Marchetti M. A collaborative framework for intrusion detection in mobile networks. Information Sciences. 2015; 321:179–92.

14. Subba B, Biswas S, Karmakar S. Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation. Engineering Science and Technology, an International Journal. 2016; 19(2):782–99.

15. Krishna P, et al. A cluster-based approach for routing in dynamic networks. ACM SIGCOMM Computer Communication Review. 1997; 27(2):49–64.

16. Mohammed N, et al. Mechanism design-based secure leader election model for intrusion detection in MANET. IEEE Transactions on Dependable and Secure Computing. 2011; 8(1):89–103.

17. Savasere A, Omiecinski ER, Navathe SB. An efficient algorithm for mining association rules in large databases. ACM Digital Library; 1995. p. 432–44.