Co-operative IDS Architectures for MANETs - A Survey

Kapil Dhamecha
Department of Computer Science,
Rollwala computer center,
Gujarat University,
Ahmedabad,
India

Rutvik Upadhyay
Department of Computer Science,
Rollwala computer center,
Gujarat University,
Ahmedabad,
India

Bhushan Trivedi, PhD.
GLS institute of computer tech,
Ahmedabad, Gujarat,
India

ABSTRACT
There are many IDSs (Intrusion Detection System) which are working on wired networks, but for MANETs we do not find any single application that can be applied directly. Different characteristics of MANET make the conventional IDSs ineffective and inefficient for the wireless environment. MANET is a combination of nodes with limited power, bandwidth and processing capability. In MANETs, an intrusion detection task performed by a single node reduces power level drastically in no time. Because of power constraints, we have to distribute the task among several nodes so that we can uphold the power level of legitimated nodes. In this paper we evaluate different performance parameters of distributed and cooperative IDSs and we also try to figure out which parameters are detracting, such as accuracy ratio, false positive and false negative detection ratio, node mobility, type of threat model and the complexity of the algorithm etc.

Keywords:
Intrusion detection system (IDS), Mobile Ad-Hoc network (MANET), Co-operative architecture

1. INTRODUCTION

Basically, there are three types of IDSs characterized for MANETs – (i) based on architecture, (ii) based on detection method and (iii) based on data collection method. An architecture based IDS illustrate the structure of operation used in MANETs. Data collection technique illustrates how data are collected and interpreted. The detection technique shows the detection mechanism to find vulnerabilities in the host as well as in a network.

An architecture based IDSs are classified in (a) stand-alone architecture, (b) distributed & co-operative architecture (c) hierarchical architecture [4]. In standalone architecture, intrusion detection task is limited to single node detection and detection is executed independently for each node. In cooperative architecture, detection task is divided among several nodes, which used to find out intrusion locally as well as globally. The hierarchical architecture is more mature cooperative architecture, where intrusion detection is performed by an IDS agent within the cluster and managed by the cluster head.

Detection based IDSs are categorized as (a) signature based and (b) statistically anomaly based. In the signature based detection method, prior knowledge of the signatures of the known attacks is required. This method possesses high detection accuracy but inefficient to detect new attacks. In anomaly based detection, abnormal behavior of the node is identified by violation of defined rules.

In data collection techniques based IDSs, agents with specific task are designed and distributed among several agents including intrusion detection task and this type of approach can be used with any type of architecture and detection method like cooperative with anomaly [7] and hierarchical with the anomaly based detection method.

An IDS provides a second line of defense against a variety of attacks that can compromise the security and proper functioning of defined protocols. An intrusion detection task in MANET is very much critical because of limited resources. Thus, the detection task is divided among multiple nodes which work together to reduce the burden to a single node. The dynamic topology and decentralizing architecture of MANET help to distribute various tasks among different nodes for the detection either by locally or globally.

The intrusion detection system performance is highly affected by node mobility (no of pause time), accuracy ratio, false positives, false negatives, detection time, log file presentation, and audit data overhead. Many other parameters also affect the performance of intrusion detection system.
The figure 1 in Appendix A shows the classification of IDS based on above discussion and different approaches to cooperative architecture.

The rest of this article is organized as follows. Section 2 reviews the related work of different cooperative approaches. In section 3, we brief about comparison of different proposed approaches based on implementation environment and their results to defend the threats. In section 4, a comparison criterion is defined based on the parameters which have affected the most to the operation of IDS in MANET. In section 5, based on carried analysis we conclude about various approaches and try to find out which IDS method is most promising to implement.

2. RELATED WORK

MANETs have power, space and processing constraints, so distributed and co-operative architecture is very much convenient for MANET, where legitimated nodes accord distributed intrusion detection task, which utilizes less resources. One of the greatest advantages of this architecture is to find the intrusion locally as well as globally by collaborative decision.

Here, we only discuss the existent research work that relates to our area of research interest in intrusion detection system in MANETs.

The very first distributed and cooperative model was proposed by Zhang and Lee [15]. As the true detection rate for a single node is very low, they proposed the cooperativeness approach among the nodes to find the possible threats with high detection rate. Based on this model, many new approaches were introduced.

The **first approach** proposed by Wang et al. [12], showed, how a node in MANET made friendly affiliation (significant association) to other nodes and trust [12] each other by direct or indirect friendship making global intrusion detection prominent. Similarly, Razak et al. [6] proposed trust based IDS which had mainly focused on global detection of intrusion considering large MANETs.

The **second approach** was proposed by Bose et al. [2]. In this author focused on multi-layer detection such as MAC, network and application layer. Each layer had introduced its own detection engine for local detection and cross layer approach for global detection. Similarly, Komninos and Douligeris[4] proposed layered intrusion detection system based on two layers : MAC and network. However the attacks at the transport layer and application layer remained undetected. Sun et al. [9] proposed similar approach addressed only disruption attacks at the network layer.

In **third approach** proposed by Ramachandran et al. [7] based on agents, which basically tried to balance the load of IDS among participating nodes.

3. IMPLEMENTATION ENVIRONMENT AND CONSEQUENCES:

3.1 Trusts based co-operative IDS

In trust based IDS, nodes form mutual trust or mutual bonding in between through the network.

3.1.1 Social network based cooperative IDS [12], the authors have evaluated the proposed approach based on NS2 network simulator with 30 nodes, two tiers and three modules for anomaly detection. This approach introduces real time trust or friendship between nodes in MANETs with three anomaly detection modules. In simulation authors have performed an operation with different transmission range varying from 100m to 250 m where any one random node performs Black hole attack and other node performs sleep deprivation attack. In one scenario, the comparison is made for the attack being detected by a single node and by multiple nodes. Their detection ratios and false positive ratios are also measured. In the other scenario, the author compares the results with associated rule mining algorithm, along with detection ratios and false positive ratios. Finally they have proven that social networking works well under the mentioned scenarios, which is also quite simple and easily understandable. A non-neighbor also contributes in detection process based on social relationship with other nodes.

Attacks addressed: Single node Blackmail, Packet dropping, Black hole, Sleep deprivation attack

3.1.2 Friend assisted cooperative IDS [6], the authors have evaluated the proposed approach based on *NS2* network simulator with 30 nodes, two tiers and seven modules for anomaly detection. It includes two separate modules for a signature and anomaly detection. Thus, this approach also stores predefined signatures of attack. The dynamic signature updating is also carried by the console which later distributed to other nodes. One of the advantages of this approach is to defend against single blackmail attacker and colluding blackmail attacker.

The analysis is carried with 2 different scenarios and 4 tests for global detection, one with less dense nodes (university campus) and other with more dense nodes (city). They have also evaluated the performance of the friend filtered algorithm and the voting algorithm.

In the **First** test, authors compare the results by finding the number of normal and abnormal activities in both scenarios but they fall behind the voting algorithm while using the friend filtered algorithm.

In the **second** test, the authors try to defend the single or colluding blackmail attacks. This time they very much succeeded with nearly 100% accuracy and zero false alerts [6].

In the **third** test, they try for a better global detection. They compare friend filtered global detection algorithm result with a voting global algorithm for colluding blackmail attack. In the less dense area the attacker node has to travel more to send fake messages to the others. Thus, with the less dense area, blackmail attack itself becomes weaker.

In the **fourth** test, the authors try to measure the effectiveness of their algorithm to prevent nodes from receiving false alerts from the neighbors. In this case, the authors also have made an assumption that all trusted nodes are well behaved nodes.If more number of trusted friends are present in the network then the performance will be much better than the voting algorithm.

The essential factor that really matters in a friendship based IDS is an initial trust i.e. how a new node can be trusted by others when it initially comes in the range of each other? For this, the authors declared 5 nodes as trusted nodes. The audit data are accepted only by the trusted ones and from those which are being trusted by the declared nodes through the self-experience and the self-observation. This approach introduces real time analysis to find suspicious activity at an earlier stage.

Attacks addressed: Single & Colluding Blackmail attack.

3.2 Agent based co-operative IDS

3.2.1 FORK agent based cooperative IDS [7], the authors have evaluated the proposed approach based on real time analysis with two tier and eight modules for anomaly detection**.** This approach divides the work into two parts:

1. Based on the power level, where nodes do auction to participate in detection task and the most reputed nodes (sufficient power level) are allocated the work. Here,

the authors have also modified the power calculation formula, called as a PLANE [10].

2. Knowledge collection from other nodes to identify anomaly detection.

In simulation, the authors perform various operations on different algorithms like Kachirski et al. [3], FORK, SPAID [10] and ATLAS [11]. They are tested on different ratios of battery power per agent and the optimal battery power, required to accomplish the task. They have also considered the different types of audit data like mail, domain files and other files which are collected from the server and applied to fork algorithm for predicting the detection accuracy within the rules. They have also noted that the fork algorithm has shown greater predictive accuracy than C5 algorithm [16] and has outperformed the Ant Miner with less number of rules and least ratio generated according to audit data collection [7].

Attacks addressed:DOS attack, Route modification attacks

3.3 Layered co-operative IDS

This type of IDSs focus on anomalies affecting many layers like physical, data link, network, transport and application layer [4]. However, most of the attacks affect the data link and the network layer due to routing and access control. MANETs highly depend on these layers' protocols where all routing and media accesses are controlled by these layers. This is also referred as cross layer detection where one layer module forwards results to another layer for better results.

3.3.1 Multilayered IDS [2], theauthors have evaluated the proposed approach based on Glomosim 2.03 simulator with single tier three modules architecture based on a 2000 x 2000 meter flat space and 30 mobile nodes. Individual module is allocated for three different layers such as MAC, network layer and application layer. Five types of detection modules (MAC, NETWORK, APPLICATION, LACE and GACE) are utilizedand each module measures the percentage of detection rates and false positive rates in each module. Simulation result shows that the application layer detection ratio is the highest compared to other layers.

Attacks addressed: DoS attacks

*3.3.2 Routing anomaly based IDS [8],*the authors have evaluated the proposed approach based on Glomosim 2.03 simulator with a single tier, two module architecture based on a 1000 x 500 meter flat space and 30 mobile nodes.This approach mainly focuses on network layer for route disruption attack. The authors have defined two parameters: PCR (percentage of change in route entries) and PCH (percentage of change in number of hops) to find malicious activities with DSR protocol. In DSR, the source transmits packet with full route information to reach the destination, so this IDS mainly focuses on fields which are altered in route path.

Attacks addressed: Route modification attack (Byzantine attack, replay attack)

3.3.3 Layered IDS framework [4], the authors have evaluated the proposed approach based on NS2 simulated with single tier three module architecture. This IDS mainly focuses on the link layer and the network layer. Various operations on different protocols (AODV, DSR and DSDV) with different simulation times have been carried and the best detection rate accuracy is found in DSR compared to AODV and DSDV. In all cases the false alarm rate remained constant even in the case of different mobility.

Attacks addressed: Route logic disruption, DoS attack, traffic pattern distortion.

4. COMPARISON CRITERIA

IDS mainly depends on accuracy of generating true alarms when actual attack has happened, but still no perfect IDS exists with zero false positive and zero false negative.

4.1 Detection Accuracy with complexity of algorithm

The detection accuracy also much depends on the type of algorithm used for detection, so we try to address both accuracy and complexity. Generally, higher complex algorithm has higher accuracy, but due to power constraint less complexity algorithm with higher accuracy is more preferred in MANETs.

4.1.1 Less complexity of algorithm with high detection rate

- **Social network based IDS [12]** uses Freeman General Centrality and Social Matrix scheme. Both are less complex because centrality mainly depends on the closeness and the vicinity of the nodes which is easily achieved by sharing trust table. Thus the accuracy of this algorithm is higher compared to other anomaly detection engine, but it might be affected by higher mobility.
- **Fork agent based IDS [7]** uses ACO (Ant Colony Optimization) algorithm which is less complex since the rules are formed based on Association Rule Mining technique. The ACO algorithm is used to gather knowledge from log files and session files, and then they classify and construct a prediction model with higher accuracy of intrusion detection.
- **The layered intrusion detection framework IDS [4]** uses Lagrange Interpolation techniques in which algorithm work on linear threshold scheme. This scheme is mainly applied to the allotment of secret shares to a set of shareholders, which is a linear combination. Thus, the complexity is less with high accuracy.

4.1.2 High complexity of algorithm with high detection rate

- **Friend assisted IDS [6]** uses friend filtered detection mechanism, which has a higher complexity since the architecture has 8 different stages and data pass through each stage. It also checks the signature and anomaly based intrusion, so mechanism itself is very complex as finding a pattern of any attack is a critical task in MANET. This mechanism has a high rate of accuracy with high rate of detection.
- **Routing anomaly based IDS [8]** usesa Markov chain model which making chain of states, where current state depend on the previous state with a finite number of states. In MANETs to maintain states itself a crucial task so algorithm accuracy very much higher with higher complexity.

- **Multi layered IDS [2]**usesa Cross feature technique, Markov chain model algorithm, confidence level threshold, and data-mining algorithm for different layers. Each layer has a detection engine with proposed algorithm. For global detection the cross layer feature is also used.

4.2 Audit data representation

Here, the audit data stand for log files and session files. For better results, audit logs exchange between the nodes. Some approaches shows underperform due to periodic exchanges and event trigger updates, and others use the whole log file or only the result of the audit data, which is actually filtered out locally. This overhead somehow affects the performance of the network.

- **Social network based IDS [12]** usesMAC and routing layer tables as audit data, which are exchanged based on the relations between the nodes.
- **Friend assisted cooperative IDS [6]** uses only locally summarized audit data which are exchanged between the friend nodes, where audit data again summarized locally, and if there is any intrusion footprint found, one can alert neighbors.
- **FORK agent based cooperative IDS [7]** uses session files and log files as audit data, which are exchanged between agents.
- **Multilayered based IDS [2]** usesa different audit data form for different layers. In MAC layer Normal profile is created using the threshold value. If such value is beyond the threshold, that will notify to neighbor nodes. The same criteria apply at the network layer which monitors number of routes selected and number of hop count fields. The application layer uses the source node, the destination node, and the packets received fields.
- **Routing anomaly detection and Layered intrusion detection framework [8]** usesvector quantization which generates the discrete data in the form of codebook size and the source vector as audit data. Audit data exchange among the nodes where each node forms a tree for the network. If any attack strikes, the nodes transfer only the coordinates with a blank child node.

4.3 Node mobility & Simulation time

Mobility of the node is related to node's speed and number of pause times for simulations in MANETs [6]. The mobility of the node during the measurement of parameters needed for the intrusion detection computation can cause inaccuracies in the estimated results and also introduces more irregularities in the gathering of data for IDS. In some cases we have observed that the false positive rate is increased with high mobility, which introduces more unexpected changes in the performance.

The simulation time is the most crucial parameter for evaluation [1, 2, 3, 4, 5, and 6]. MANET topology is dynamic in nature. So, the node position changes with speed. This causes irregularities to the performance of the IDS.

- ***Social network based IDS [12]*** uses minimum node speed of 1 m/s to maximum speed of 5m/s with no of pause times as 10/100/300/1000 seconds in 30 minutes simulation time. However, there is no difference in the detection accuracy and the false alarm ratio due to these different mobility patterns.
- ***Routing anomaly based IDS [8]*** uses minimum node speed of 3 m/s to maximum speed of 5m/s with no of pause times as 30/150/300/600/900 seconds in 400 minutes simulation time. In this scenario, more irregularities are found in the detection accuracy and in the false alarm ratio, as this approach considers the node speed as one of the feature of detection rules.

5. CONCLUSION

This paper evaluates and compared the most prominent distributed and cooperative IDS architectures for MANETs along with performance aspects and significant limitations.

Table 1 (Appendix A) shows that most of the cooperative architectures can identify a limited set of attacks due to lack of certainty between nodes. Researchers have cogitated for several mechanisms that suited to MANET environment. For example, authentication schemes, secure route protocols, cooperation enforcement and inclusion of CA (Certificate Authority) mechanisms [13] etc. but all the mechanisms have failed to restrain the attacks. We summarized all the distributed and co-operative IDSs (Appendix A), where intrusion detection task equates the load among several nodes which saves battery power, reduces processing overhead and bandwidth consumption. The friendship mechanism appeals more since the credence of the nodes is based on the relations between them. Thus, we have focused on social networks based [12] as well as friend assisted based IDSs [6]. In both the approaches authors allude to the malicious behavior of the node which is monitored by the association between the nodes. Meanwhile, low processing overhead and high accuracy with low complexity has been achieved. It is a concept of mutual friends (friends of friends), where each node tries to maintain the trust and also helps to measure the trust to any new node who wants to join the network. This is actually very conducive to find the behavior of any node, which reduces the risk of possible threats to a network. We therefore plan to build a mechanism where initial trust may be built according to a study of the neighbor node profile. The audit data overhead in [1, 3, 4, and 5] is very much higher compared to multilayered IDS [2] since it exchanges only locally analyzed data. The node mobility and the simulation time are the performance deciding factors which concede during the implementation.

The future direction includes expansion of the social networking approach that can focus on misbehaving attacks such that the approach would be the best fitted as cooperative as real time social networking among friends.

6. REFERENCE

[1] Albers P, Camp O, Percher J., Jouga B, Me L, Puttini R. , 2002:Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches, *Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002)*, pp. 1–12

[2] Bose S, Bharathimurugan S, Kannan A, February 2007, :Multilayer Integrated Anomaly Intrusion Detection System for Mobile Ad Hoc Networks, *IEEE ICSCN 2007*, MIT Campus, Anna University, Chennai, India, pp.360-365.

[3] Kachirski O, Guha R.K, *2003*: Effective intrusion detection using multiple sensors in wireless ad hoc networks, *Proceedings of HICS, 57*

[4] Kazienko P., Dorosz P: *Intrusion detection systems. Part I. Intrusion types and symptoms. Tasks and architecture of IDS*. Translation from Polish , IT FAQ 12/2002, pp. 21-27

[5] Komninos N, Douligeris C, January 2009 : LIDF: Layered intrusion detection framework for ad-hoc network, *Elsevier Ad Hoc Networks*, **vol. 7**, issue 1, pp. 171 – 182,

[6] Razak S.A., Furnell S.M., Clarke N.L., Brooke P.J., September 2008: Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks, *Elsevier Ad Hoc Networks*, **vol. 6**, issue 7, pp. 1151 – 1167.

[7] Ramachandran C, Misra S, Obaidat M, October 2008: FORK: A novel two-pronged strategy for an agent based intrusion detection scheme in ad-hoc networks, *Elsevier Computer Communications***, vol. 31**, issue 16, Performance Evaluation of Communication Networks (SPECTS 2007), pp.3855-3869.

[8] Sun B., Wu K., Pooch U. W , 2003: Routing anomaly detection in mobile ad hoc networks, *IEEE International Conference on Computer Communications and Networks*, (ICCCN'03), pp. 25-31.

[9] Sun B, Wu K., Xiao Y, Wang R, June 2007: Integration of mobility and intrusion detection for wireless ad hoc networks, *Wiley International Journal of Communication Systems,* vol. 20, issue 6, pp. 695 – 721.

[10] Srinivasan T., Seshadri J., Sidharth Jonathan J.B., Chandrasekhar A, august 2005 : A system for power aware intrusion detection in wireless ad-hoc networks, *Proceedings of Third International Conference on Computer Networks and Mobile Computing, ICCNMC 2005*, Springer Verlag, Berlin, Heidelberg, 2005, pp. 153–162. LNCS 3619, Zhangjiajie, China,

[11] Srinivasan T, Vijaykumar V, Chandrasekar R, 2006 : An auction based task allocation scheme for power-aware intrusion detection in wireless ad-hoc networks, *Proceedings of the Third International Conference on Wireless and Optical Networks*, IEEE, Bangalore, India

[12] Wang W., H. Man, Y. Liu , April, 2009: A Framework for Intrusion Detection Systems by Social Network Analysis Methods in Ad Hoc Networks, *Wiley Security and Communication Networks*, **vol. 2**, issue 6, pp. 669 – 685.

[13] Wireless Security Workshop, Sep2002 :*WiSe'02 workshop on wireless security*, Atlanta, pp. 11–20.

[14] Yang, Meng X., Lu S,2002: Self-organized network-layer security in mobile ad hoc networks", *wise 02 proceeding of first acm workshop on wireless security*, pages 11-20

[15] Zhang Y, Lee W, Huang Y :A Intrusion detection techniques for mobile wireless networks, *Wireless Network* 9 (5) (2003) 545–556.

[16] Zhang R., 2004Using constructive induction to enhance the predictive accuracy of the c5 machine learning environment, *Proceedings of IC-AI*, pp. 1117–112.

Appendix A:

Co-operative IDS						
Comparative parameter	**Social network analysis based**	**Friend assisted based**	**Fork (agent) based**	**Multilayer based**	**Routing anomaly based**	**Layered intrusion detection framework**
No of Modules	Three	Seven	Eight	Three	Two	Three
Architecture type	Single tier	Two tier	Two tier	Single tier	Single tier	Single tier
Audit data	Mac and routing layer table are exchange	Only locally summarized audit data are exchanged	Session files and log files are exchanged	Only Cross feature of layer are exchange	Collect data from all the node	Features of each layer are selected and exchange
Complexity of detection	Very Less	Very high	Less	High	Very high	Less
Accuracy of detection	High	High	Very high	High	Very high	High
Types of detection engine	Anomaly based detection	Misused + Anomaly based detection	Anomaly based detection	Anomaly based detection	Anomaly based detection	Anomaly based detection
False positive	High	Very low	High	Low	Low	High at particular layer
Overhead in network	High due to audit data exchange	High , due to audit data exchange between nodes	High , if node mobility is high	Low, only detection results exchange	High, if engines hosted at neighbor nodes	Low
Base protocol for simulation	AODV	Not specified	Not specified	DSR	DSR	AODV, DSR, DSDV
Simulation tool	NS2	NS2	REAL TIME ANALYSIS	Glomosim 2.03	Glomosim 2.03	NS2
Speed of node in simulation	Min -1m/s Max -5m/s	Not defined	Not defined	Not defined	Min - 3m/s Max - 5m/s	Not defined
Mobility (no of pause time in seconds)	10,100,300,1000	Not defined	Not defined	Not defined	30,150,300,600,900	Not defined
Main purpose	To make Simpler implementation and lower complexity than other anomaly IDS	Better Global detection of intrusion	IDSs processing load sharing	Better decisions based on cross layer feature	To find Cross layer anomalies in layers	To check route logic compromise, trafficpattern distortion and denial of service attacks

Table 1: Comparison of Co-operative architecture based intrusion detection systems

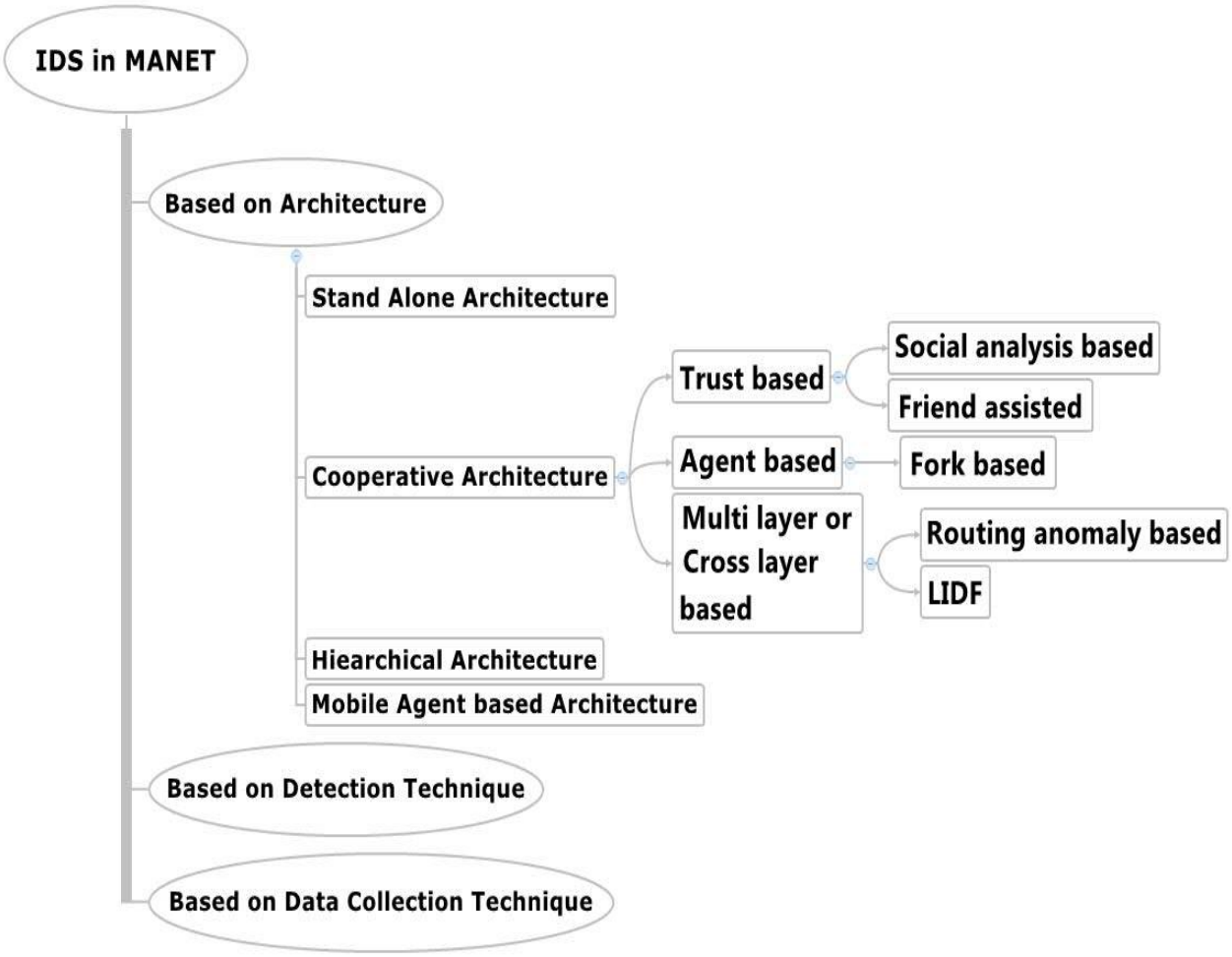

Figure 1: Classification of IDSs based on cooperative architecture.