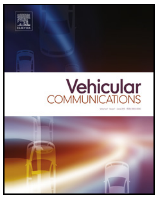
Contents lists available at ScienceDirect
Vehicular Communications
www.elsevier.com/locate/vehcom



Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET

Sparsh Sharma, Ajay Kaul

Department of Computer Science and Engineering, Shri Mata Vaishno Devi University, Katra, India

ARTICLE INFO

Article history:
Received 7 July 2017
Received in revised form 9 September 2017
Accepted 12 December 2017
Available online xxxx

Keywords:
AHP
Dolphin Swarm Algorithm (DSA)
Intrusion Detection System (IDS)
MCDM
Support Vector Machine (SVM)
TOPSIS
VANET

ABSTRACT

Existing Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) based communication suffers from various security and performance issues, hence Cluster based Communication is preferred nowadays. However, Cluster based Communication adds extra overhead and burden on the Cluster Head (CH) in dense network scenarios which eventually introduces delay and hinders network performance. To reduce the overburdening of single CH, a multi cluster head scheme is proposed in which multiple nodes in a cluster can act as CH to share the load of single CH. For a selection of stable CH, Hybrid Fuzzy Multi-criteria Decision making approach (HF-MCDM) is proposed in which Fuzzy Analytic Hierarchy Process (AHP) and TOPSIS methods are clubbed together for optimal decision making. Further because of association of Vehicular Ad-hoc Network (VANET) with life-critical applications, there is a dire need for a security framework to detect various malevolent attacks. Machine Learning based Intrusion Detection System (IDS) like Support Vector Machine (SVM) is one of the approaches for curbing such attacks. These intrusion detection based mechanism can be combined with various existing optimization techniques to improve their performance, and Dolphin Swarm Algorithm is one such approach. Dolphins have many significant biological features like echolocation, exchange of information, coordination, and division of labor. These biological features combined with swarm intelligence can be utilized for optimizing the detection and accuracy of SVM based IDS. So in this paper, a Multi-Cluster Head anomaly based IDS optimized by Dolphin Swarm Algorithm has been proposed and its results are compared with various existing Security frameworks in terms of parameters like false positive, detection rate, detection time, etc. and it is observed that the proposed approach performs better.

1. Introduction

Deploying Intrusion Detection System (IDS) for traditional networks and Vehicular Ad-hoc Network (VANET) based systems are somehow different. Various factors like limited power, storage and computational capability in nodes need to be considered [7]. Unlike traditional IDS, VANET based IDS needs to be deployed carefully in such a way that their operation should not hinder the real time performance of VANET applications. Fig. 1 shows classification of different types of IDS used in VANETs.

There exist numerous IDS based solutions for VANET in literature. Some of them use rule based while the others use threshold based detection [10]. The majority of them, however, have problems like low detection rate, high false positives, high detection time, added overhead on the network, etc., associated with them. Rule based detection is good for existing attacks only, whose signature patterns are in the rule database. However, it is not capable of detecting newer and modified attacks. Anomaly based IDS has advantages over the rule based IDS in the way that it is capable of detecting even newer attack whose signature is not present in the database [13]. But this category of IDS requires setting of an optimal threshold and huge training set for making it capable to differentiate between the malicious and normal nodes. Table 1 gives a comparative analysis of various existing IDS techniques in VANET.

So keeping aforesaid problems in consideration, we have developed a lightweight Dolphin Swarm optimized anomaly based IDS with high accuracy and low detection overhead.

Also to counter confidentiality and integrity based attacks, various cryptographic solutions are available in literature [16,17] but these solutions add to the network delay for exchange and processing of private/public keys, so Dynamic Trust Attribute Based Encryption (DT-ABE) is used in our proposed framework to tackle the above attacks and to reduce the extra processing and decryption delay. DT-ABE reduces the number of steps in encryption and decryption of the message and eliminates the requirement of any centralized Trusted Authority to be online all the time.

E-mail address: sparsharma@outlook.com (S. Sharma).

https://doi.org/10.1016/j.vehcom.2017.12.003
2214-2096/© 2018 Elsevier Inc. All rights reserved.

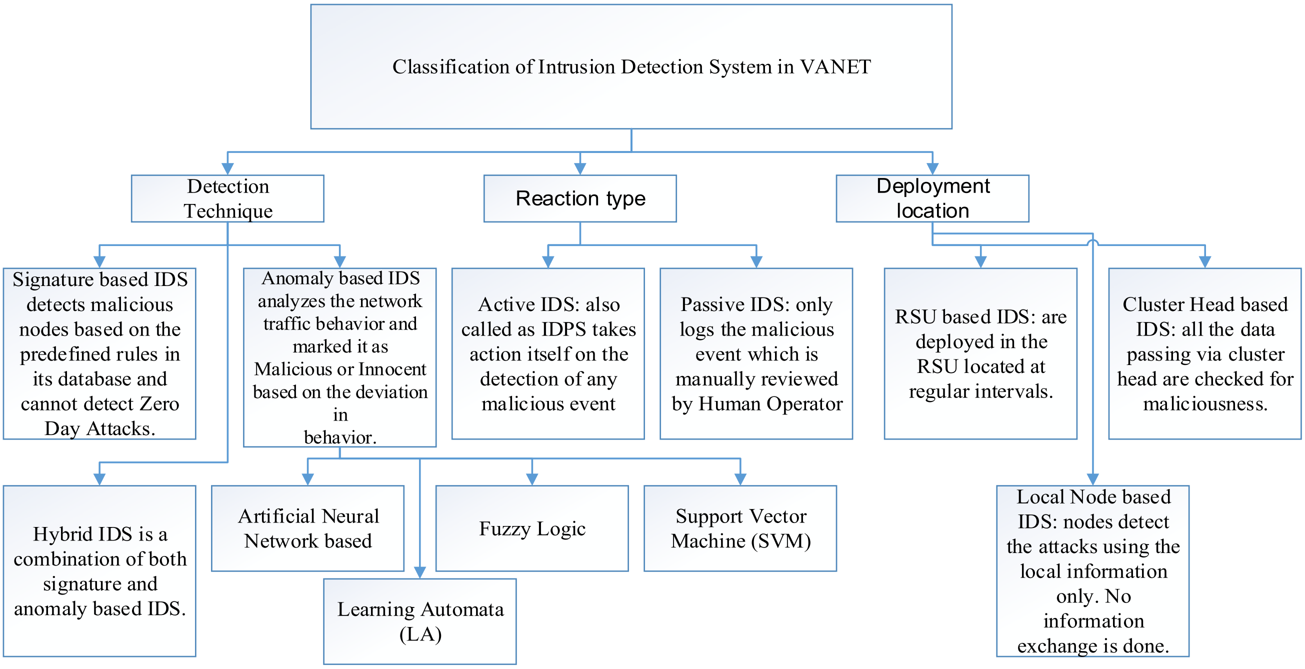

Classification of Intrusion Detection System in VANET
Detection Technique
Reaction type
Deployment location
Signature based IDS detects malicious nodes based on the predefined rules in its database and cannot detect Zero Day Attacks.
Anomaly based IDS analyzes the network traffic behavior and marked it as Malicious or Innocent based on the deviation in behavior.
Active IDS: also called as IDPS takes action itself on the detection of any malicious event
Passive IDS: only logs the malicious event which is manually reviewed by Human Operator
RSU based IDS: are deployed in the RSU located at regular intervals.
Cluster Head based IDS: all the data passing via cluster head are checked for maliciousness.
Hybrid IDS is a combination of both signature and anomaly based IDS.
Artificial Neural Network based
Fuzzy Logic
Support Vector Machine (SVM)
Learning Automata (LA)
Local Node based IDS: nodes detect the attacks using the local information only. No information exchange is done.

Fig. 1. Classification of IDS in VANET.

There are three main types of communication possible in VANET: a) Vehicle-to-Vehicle (V-2-V), b) Vehicle-to-Infrastructure (V-2-I) and c) Hybrid. But these existing communication types suffer from various disadvantages such as large number of Road Side Units (RSUs) are needed at regular locations in V-2-I communication which are not financially feasible, privacy and security issues in V-2-V based communications [19], so clustering communication is preferred nowadays which has advantages over the above three communication types [21]. But in clustering based communication all the communication occurs through the Cluster Head (CH) only i.e. if node A in cluster 1 wants to communicate with Node B in cluster 2, then first the message from node A will be sent to CH of Cluster 1 and from that CH to CH of Cluster 2 and finally to the node B. This approach in highly congested traffic scenarios adds extra load on the CHs which eventually introduces delay in the communication and affects the whole network performance. So to deal with this, a new clustering architecture inspired from dolphin swarm behavior has been proposed in this paper in which multiple nodes can act as a CH in a cluster and thus can share their load in heavy traffic scenarios improving the whole network performance.

1.1. Motivation

A lot of security proposals are available in literature that claims to enhance the security of VANETs but at the cost of hindered network performance. So there is a requirement of a security solution that enhances the security of VANET but not by degrading the network performance. Various IDS solutions are proposed by researchers in literature but most of them uses complex and heavy detection strategy that require huge network resources and computation for the detection of malicious nodes. So in this research article, a lightweight IDS has been proposed that provides improved false positive and detection rate along with low detection time.

Also, since in cluster based communication, cluster heads (CHs) are made responsible for all the communication to and from within a network. So in highly dense network scenarios, CH can easily get overburdened and can lead to delay in decision making and degraded network performance. So a concept of Multi-Cluster Head inspired from dolphin load sharing behavior has been proposed in this article in which multiple nodes can act as CH in a single cluster to share the node of single CH.

For selection of optimal and secure CHs in clusters, Hybrid Fuzzy Multi Criteria Decision Making (HF-MCDM) approach has been proposed in which various important criteria for CH selection are being considered, and every non malicious nodes are assigned ranks using it. So if any node which is non malicious and has a rank value equal or greater than the specific threshold is made as another CH.

1.2. Contributions of this article

1) A Lightweight anomaly based IDS optimized with Dolphin Swarm Algorithm has been proposed for the detection of malevolent attacks in VANET.
2) Proposed IDS utilizes the Dolphin Swarm behavior of hunting and praying for detection and isolation of malicious nodes from the network.
3) For improved network performance and reducing the CH load in dense network scenarios, the concept of Multi-Cluster head in single cluster has been proposed.
4) For a selection of optimal CH, Hybrid Fuzzy based Multi-criteria decision making (HF-MCDM) approach has been proposed in which Fuzzy AHP method has been utilized for weight determination of the criteria and Fuzzy TOPSIS method has been utilized for CH Selection decision making.
5) Existing Dynamic Trust Attribute Based Encryption (DT-ABE) is modified with extra trust metrics for providing secure data dissemination.

Remaining paper is organized as follows: Section 2 gives a brief overview of the related literature of this work. Section 3 presents details of our proposed security framework. Section 4 discusses advantages of using the Proposed Security Framework, and security overview of the proposed security framework is provided in Section 5. In section 6, Performance and Evaluation results are provided. Finally, Section 7 gives the concluding remarks of this paper along with its future scope.

Please cite this article in press as: S. Sharma, A. Kaul, Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET, Veh. Commun. (2018), https://doi.org/10.1016/j.vehcom.2017.12.003