International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

A Collaborative Intrusion Detection System for Cognitive Radio Networks with Trust and Reputation Management

S. Sankar Ganesh, K. Somasundaram

Abstract: ***Systems administration cognitive radios and hubs from primary system (PS) results in a heterogeneous existing together multi radio remote system, with the goal that critical system throughput addition can be accomplished. Be that as it may, by exploring cognitive radio networks (CRN) engineering, the connections in CRNs are probably not going to help total security check because of connection elements, crafty accessibility, and uni-directional in accessible time window, so trust and reputation system is required. CORE is a reputation based security mechanism which enforces cooperation of nodes in CRN. CONFIDANT is based on selective unselfish and belief in mobile nodes and it aims to detect and isolate misbehaving nodes. Both CORE and CONFIDANT mechanism give the trustworthiness of all mobile nodes in the network and it punishes misbehaving nodes once it detected. This paper gives the comparative study of trust based neighbor monitoring CORE and CONFIDANT on secured routing protocols. The simulation results shows that our work provides better detection efficiency, better detection coverage and packet delivery ratio in routing protocols with neighbor monitoring scheme.***

Index Terms: CRN, Core, Confidant, Trust, Reputation

I. INTRODUCTION

Cognitive radio is broadly expected to be the following huge explosion in remote interchanges. Range administrative Boards of trustees in numerous nations have been finding a way to open the way to dynamic range get to utilizing this innovation and furthermore setting out the principles for its usage. Worldwide associations have likewise been taking a stab at institutionalizing and harmonization this innovation for different applications. This report reviews meaning of Cognitive radio frameworks and portrays the condition of craftsmanship in the administrative and institutionalization exercises on Cognitive radio everywhere throughout the world, which are regarded to have primary impact on the eventual fate of remote correspondences.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
S. Sankar Ganesh*, Research Scholar, Department of CSE, Vinayaka Mission's Research Foundation, Salem, Tamil Nadu, India. E-mail: seeniganesh1984@gmail.com.
Dr. K. Somasundaram, Professor, Department of CSE, Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation, Salem, Tamil Nadu, India. E-mail: soms72@yahoo.com.

Cognitive radio ideas can be connected to an assortment of remote interchanges situations, a couple of which are portrayed here.
Cognitive radio ideas can be connected to an assortment of remote correspondences situations, a couple of which are portrayed in this archive furthermore, the significant capacities and utilizations of Cognitive radio and segments of Cognitive radio and usage issues are surveyed. We likewise talk about the administrative issues and key ideas. At last, in view of led study through the specialized and administrative examination, a reliable end gave.
"Cognitive Radio System (CRs) is a radio system employing technology that allows the system to obtain knowledge of its operational and geographical environment, established policies and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives; and to learn from the results obtained."Cognitive radios empower the utilization of transiently unused range, alluded to as range gap or blank area, and if an primary client means to utilize this band, at that point the secondary client ought to consistently move to another range opening or then again remain in a similar band, modifying its transmission control level or adjustment plan to maintain a strategic distance from meddling with the primary client. Conventional range allotment plans what's more, range get to conventions may never again be relevant when secondary unlicensed clients exist together with primary authorized clients. In the event that secondary clients are permitted to transmit information alongside primary clients, the transmissions ought not to meddle with one another past a limit. On the other hand, if secondary clients can transmit just in the nonattendance of primary clients, at that point an optional client transmitting information without a primary client ought to have the capacity to distinguish the return of the primary client and abandon the band. There is a lot of research presently being directed and more should be performed to grow new range the board approaches identified with Cognitive radio for both range detecting and dynamic range sharing. A Cognitive radio system engineering incorporates segments comparing to both the secondary clients (optional system) and the primary clients (primary system).

The secondary organize is made out of a lot of optional clients with or without an optional base station, all of which are furnished with CR capacities optional system with a base station is alluded to as the foundation based CR organize;
the base station goes about as a centre point gathering the perceptions what's more, aftereffects of range investigation performed by every CR optional client and choosing how to stay away from obstruction with the primary systems as shown in Figure 1. According to this choice, every CR secondary client reconfigures his correspondence parameters. A secondary system without a base station is alluded to as the framework less– intellectual radio specially appointed system (CRAHN). In a CRAHN, the CR secondary clients utilize collaboration plans to trade privately watched data among the devices to widen their insight on the whole system, and choose their activities based on this apparent worldwide information. A primary organize includes primary clients and one or progressively primary base stations, which are all in general not furnished with CR capacities. Subsequently, in the event that an secondary system shares an authorized range band with an primary system, the secondary system is required to be capable identify the nearness of a primary client and direct the secondary transmission to another accessible band that won't meddle with the primary transmission. The opportunistic access of the range white space and exchanging of the recurrence groups by a CR optional client at the rate of utilization by a primary client.

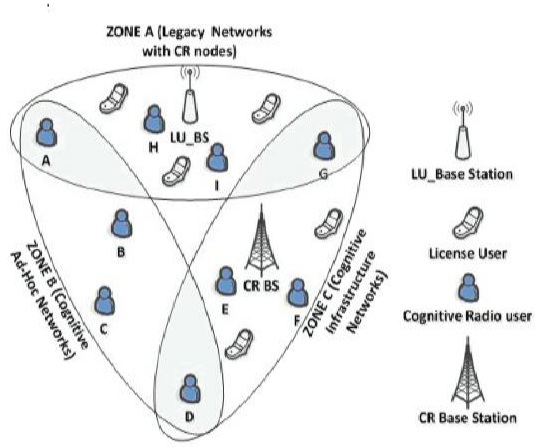

Fig 1: Cognitive Radio Network Architecture

Security is an important aspect in CRNs and the most challenging issues in this kind of networks. This paper gives the comparative study of two trust and reputation management schemes (CORE and CONFIDANT), to overcome the attacks in routing protocol. These trust and reputation schemes are implemented over multicast routing environment in routing and packet forwarding operations. During the routing process the system has to find out most trusted nodes to make a network and on this process more number of nodes will available and the system will find it difficult to select the correct nodes with the shortest path, for this issues profile based neighbor-monitoring schemes are implemented in the CORE and CONFIDANT. In the profile based neighbor-monitoring schemes each and every node will builds and maintains a profile for each of its neighboring nodes. Based on the information stored in the profile, makes the network to select an appropriate feature during the routing.

The advantage of implementing neighbor-monitoring scheme in CORE and CONFIDANT will avoid the excess amount of nodes selected for routing and it will decrease the time taken for the network on finding out those nodes. Network monitoring schemes improves the performance of the overall network and it improves the efficiency of the network detection coverage. CORE is a trust-based collaborative reputation mechanism to enforce cooperation of mobile nodes in the networks. CORE is a distributed, symmetric trust based reputation model specially designed for CRNs, which uses both the direct and second-hand information from the neighboring nodes for updating the reputation values. It is easily integrated in any of the network and network functions. Furthermore CORE scheme uses watchdog mechanism for monitoring the intermediate nodes in the network, the monitored information about the nodes is stored in reputation table. If any node has negative reputation values those nodes are prevented in the network.

CONFIDANT is also a distributed, symmetric model to enforce cooperation of nodes in the mobile adhoc networks. CONFIDANT also uses both the direct and second-hand information from the neighboring nodes for updating the reputation values in the reputation table. The main aim of the CONFIDANT mechanism is to detect the malicious nodes if any presented in the network and to punish them. CONFIDANT has four components, the monitor, the reputation system, the trust manager and the path manager.

A. Collaborative Intrusion Detection System

The idea of versatile hubs portability in Cognitive radio networks needs an extra instrument for giving security because of this a remote systems are considered as more helpless than wired systems. The conventional method for ensuring such a remote systems with firewalls and encryption programming is never again adequate because of the properties of CRNs and we have to build up another engineering and instruments for securing the subjective radio systems. In this paper we examine a community oriented interruption identification framework Intrusion detection system (IDSes) recognize interruption in the system by looking at the discernible conduct against suspicious examples. IDSes can be of Network based (NIDS) or Host-based (HIDS). A conventional IDSes work in disconnection and might be undermined by obscure dangers or new dangers all the more effectively. A Community oriented Interruption Discovery Framework (CIDS) portrays in this paper is an IDS organize proposed to beat the above shortcoming by having every hub IDS profit by the aggregate data, learning and experience shared by different hubs.

CIDS improves the general exactness of IDS to recognize new classes of interruptions. CIDS permits all circulated IDSes to team up and share their insight and feelings about interruptions.

B. Security Attacks in Crn

In the period of plan and investigation of secure distribution framework, trust is a significant element. Trust and security in Cognitive Radio Networks are constantly interlinked. They are supplemented and commonly comprehensive to one another. To talk about the assaults on CRN, we group them dependent on. The layers in which the assault can happen. At the Physical layer, Primary User Emulation assault (PUE), Target Capacity Assaults, Sticking, and so on are talked about. Assaults at the Network layer incorporate Spectrum Sensing Data Falsification (SSDF), Control Channel Saturation DOS Attack (CCSD), and so on. At the System layer. Flood Assault and Sinkhole Assault are talked about. At the transport layer, Lion assault is notable. A portion of these assaults may take a shot at various layers as well, for example, sticking, which can be propelled at physical or Macintosh layers.

II. RELATED WORK

The main issues in cognitive radio networks are cooperation, collaboration and misbehavior of mobile nodes in the network. A cognitive radio network relies on mobile nodes to collectively cooperate in an operation such packet forwarding and routing. Since many nodes may not cooperate in the network operations and they behave selfishly or maliciously. The selfish nodes will receives all the packets for forwarding but may not cooperate by forwarding those packets to the destination nodes to save the battery powers for their own communications and they do not directly intend to damage other nodes in the network, whereas the malicious nodes may directly intend to damage other nodes by giving some unwanted or wrong destination address. Also malicious nodes make other nodes to split from the networks by compromising it. Selfish nodes main priority is to save battery power and malicious nodes main priority is to attack other nodes while saving battery power is not their priority. One of the important challenges faced by CRN is spectrum allocation. If an entity authorized to access system resources but employs them in a malicious way is an insider attack. Many feature selection algorithm, trust and reputation management scheme are proposed, some of them are survey in this section. Manuel Gil Perz [1], Proposed a notoriety based community oriented interruption discovery arrange (RepCIDN), which depicts the structure of a communitarian IDS on a wired systems. Synergistic interruption discovery organize (CIDN) is fit for structure and sharing the community information pretty much all related cautions in the system so as to identify conveyed assaults all the more precisely. RepCIDN planned to improve the location inclusion of discovery arrange since it has number of IDN consolidated to shape CIDN. This model empowers a CIDN to recognize malevolent practices dependent on the reliability of the cautions which is determined from past connection with the system. P. Michiardi and R. Molva [2], recommended a conventional instrument (Center), a notoriety based system to authorize hubs participation in MANET. In Center, hubs invigorate participation by a collective observing methods and a notoriety component. Center can be incorporated with any of the system capacities like parcel sending, course revelation and system the executives. Notoriety is kept up in every hub by community data assembled from neighbor hubs. Center uses just the positive data given by neighboring hubs and those hubs which have great notoriety esteems are considered for systems administration activities and those which have terrible notoriety esteems are erased from the system's way. The notoriety esteem is determined by the data accumulated from every hub's rate of joint effort and collaboration. The upside of utilizing Center is that having a positive notoriety esteem, the hubs are compensated and named as great conduct and negative notoriety esteem hubs are rebuffed.

S. Buchegger and J. –Y. Le Boudec [3], proposed a trust based convention called as Friend (Collaboration Of Hubs: Reasonableness In Powerful Impromptu Systems) an augmentation to DSR steering convention. Associate goes for recognizing and detaching getting into mischief hubs in the systems, urges every one of the hubs to participate in system tasks and therefore it makes bad conduct ugly. Compatriot has four utilitarian segments depends on every hub, the screen, the notoriety framework, the way chief and the trust supervisor. Each hub in the system distinguishes its neighboring hubs whether it is a companion hub or adversary hub dependent on the trust and notoriety esteems given by the parts: the notoriety framework and way director. In the event that a hub is observed to be adversary hub way chief will dispense with those hubs in the steering way and furthermore the directing data about that hub. Compatriot has high parcel conveyance proportion even in a threatening situation and diminishes the effect of bogus indictments.

Q. He, D. Wu, and P. Khosla [4], proposed a protected and target notoriety based motivator (SORI) conspire for adhoc systems. SORI support hubs collaboration in system activity. SORI, furnished with notoriety instrument identify the narrow minded hubs in the system and rebuff them. The extraordinary highlights of the SORI conspire are, (I) the notoriety of a portable hubs is evaluated by target measures, (ii) the proliferation of notoriety is computationally-productively verifies by methods for single direction hash-chain based validation plan and (iii) the notoriety of a hubs is just spread to its neighbors yet not the whole system.

Carol J Fung, Jie Zhang [6], proposed a mark based interruption discovery framework for remote adhoc systems and furthermore explored the capacity of different remote adhoc directing conventions to encourage interruption identification when the assaults marks are known before.

S. Marti, T. J. Giuli. [7], proposed dirichlet-based trust the board for compelling Collective Interruption Recognition Systems. The exploration work depends on estimating the various dimensions of trust among IDSes as per their shared involvement.

Alongside trust the board calculation a colleague the executives calculation is proposed to permit every single IDS actualized in hubs to deal with its associates as indicated by their dependability. This methodology accomplishes solid versatility and is increasingly hearty against normal insider assaults.

Gomez Marmo [8], introduced an improved variant of Associate convention, "A Vigorous Notoriety Framework (RRS)" for portable adhoc systems. RRS is a reconsidered form, in which the creator presented a Bayesian system with beta circulation for refreshing notoriety estimation of every hub in the system. RRS utilizes both the accumulated positive and negative notoriety esteems yet just considers second-hand data for figuring trust and notoriety esteem and the direct data where not considered. The fundamental highlights of RRS is just the crisp data is traded all through the systems and RRS utilizes two unique sorts of measurements: notoriety metric used to characterize neighboring hubs as ordinary or making trouble hubs and trust metric then again orders hubs as reliable or dishonest.

P. L. Campbell. [9] proposed a trust the board conspire for host-based synergistic interruption recognition arrange, is a trust-based structure for verifying and accomplishing joint effort inside an interruption location organize (IDN). In this methodology, the creators especially characterize a trust model that permits every single IDS in collective IDS (CIDS) to assess the reliability of others dependent on their own understanding. Assessing the dependability of partaking IDSes is a significant issue since they are have based IDS. The trust model improves the strength of the community interruption recognition framework against noxious assaults and furthermore improves the execution of system.

Y. Hu and A. Perrig [10], Proposed another interruption location framework for MANETs named EAACK (Improved Versatile Affirmation), exceptionally planned and tried for MANETs. The examination work of EAACK dependent on verifying MANETs and it expresses that in an open medium the portable hubs are generally circulated. MANETs are more helpless against malevolent assaults than wired systems; for this situation it is increasingly basic for creating effective interruption identification instrument to shield from different assaults. The proposed IDS EAACK defeats the above issue and gives higher pernicious conduct identification rate.

B. Wu, J. Chen [11], proposed a convention named Confirmed Steering for Adhoc Systems (ARAN). ARAN utilizes open key cryptography components to identify and to overcome every single recognized assault. In ARAN, the creators initially portray the adventures that are conceivable against adhoc steering conventions, so as to configuration secure adhoc directing conventions, they previously characterized and recognized the heterogeneous situations that utilize adhoc directing and contrast in their security necessities, at that point they proposed a Confirmed Steering for Adhoc Systems (ARAN), that identifies and ensures against noxious assaults. With ARAN the system can almost certainly find verified courses all the more viably and productively.

R. Maheshwari [12], introduced a structure and exhibition assessment of another safe on-request directing conventions for portable adhoc systems, called Ariadne. Ariadne proposed for the issue in steering and parcel sending, and furthermore it empowers all hubs to helpfully perform in system activity. Ariadne with its execution maintains a strategic distance from assailants or traded off hubs from the system from altering positive courses comprise of completely positive hubs. Ariadne goes for anticipating expansive number of assaults types fundamentally disavowal of-administration assaults. Ariadne is increasingly productive when utilized with symmetric cryptographic systems.

Haong Lan Nguyen [14], proposed and researched a novel based convention for Security Convention for Dependable Information Conveyance (SPREAD), to upgrade and improve the information secrecy administration on portable adhoc systems. The primary of proposed SPREAD plan is to give further more assurance to verify mystery message from being hacked or being undermined when they are conveyed over the shaky systems. The essential thought of SPREAD plan is to change a verified mystery message in to a different offers by mystery sharing systems and after that convey it by means of a numerous autonomous ways to a similar goal, so that even a system with an extremely modest number of hubs can likewise think that its difficult to bargain the mystery message. SPREAD convention is more verified and the primary plan to build up this sort of convention is to improve the convention to be greater security arranged and to reinforce the information privacy in MANETs.

B. Sun; Y. Guan [15], proposes an agreeable interruption identification framework (IDS) for adhoc systems. This exploration work depends on irregularity interruption location framework. To give subtleties on assault types and wellsprings of assaults to the IDS, the creators examined on the most proficient method to improve the peculiarity recognition approach. For recognizing a few understood assaults the framework can utilize straightforward standard yet sometimes those principles were additionally giving false alerts. To defeat these kinds of cautions and to address the run-time asset requirements issue the creator proposed agreeable IDS utilizing a bunch based oddity discovery plot.

Yongguang Zhang and Wenke Lee [16], acquainted information mining innovation with interruption discovery framework which utilizes "cross-highlight examination". The between highlight relationship designs are caught on ordinary traffic utilizing the cross-include examination and those examples are put away in the system and are utilized as would be expected profiles to distinguish any deviation or any peculiarities brought about by assaults. The primary thought behind the cross-highlight examination is that, the strategy naturally builds oddity location modules where the deviations are accounted for and they are fit for identifying new assaults all the more proficiently. On incorporating CORE with CONFIDANT for comparative study the following issues are proposed, i. learns from observed behavior, ii. Learn from reported behavior. Cooperation and collaboration can be enforced only if non-cooperative nodes are known.

C. Fung, O. Baysal [19], proposed a profile-based neighbor monitoring anomaly intrusion detection algorithm. By neighboring monitoring scheme each and every nodes in the network IDS monitors its neighbor's traffic. Here some of the intrusion detection techniques are investigate and the author proposed profile-based IDS, in which each node builds a separate profile for each of its intermediate or neighbor nodes. The profiles include packet type, flow directions and sampling periods. In this approach the Markov Blanket discovery algorithm is implemented in IDS tries to decrease the number of features without affecting the detection rate when forming network routes.

G. Theodorakopoulos [23], proposed a SVM-based Rowdiness Location and Trust The executives structure (Keen) to address the security dangers which are brought about by different mischievous activities. In Savvy system, the Help Vector Machine (SVM) calculation is utilized for identifying the hub mischievous activities, and the SVM does not require any pre-characterized edge level to recognize misconduct hubs from ordinary conduct hubs. Here the SVM calculation is utilized to prepare and allocate a classifier gathering and that classifier is utilized to distinguish mischievous activities in the system. With this classifier, the mischief hubs are recognized more precisely than the limit based instrument. And furthermore with SVM, a multi-dimensional trust the board plot is connected to the system for assessing the dependability of every hub in MANET, from various and numerous points of view. The dependability of every hub depicts the adequacy of MANET.

L. Eschenauer [24], proposed a Perception based Participation Authorization in Specially appointed Systems (Sea). The primary target of Sea is to evade the trust-the executives apparatus and perceive how far the system performs by basically utilizing the immediate direct perceptions of neighboring hubs. Sea centers around the power of bundle sending and keeping up the general parcel throughput within the sight of getting out of hand hubs in the adhoc systems and furthermore Sea centers around two kinds of directing bad conduct: deluding and narrow minded. Sea, which is executed in every hub, has 5 parts: the NeighborWatch, the RouteRanker, the Rank-Based Directing, the Pernicious Traffic Dismissal and the Additional opportunity System. Every one of those parts perform various capacities to distinguish and alleviate acting mischievously and narrow minded hubs.

III. ARCHITECTURAL DESIGN

Figure 2, shows the architecture diagram of collaborative intrusion detection system (CIDS) with trust management system. Trust management system is combined with reputation schemes of CORE and CONFIDANT. Our CIDS framework implemented in HIDS (Host-based Intrusion Detection System) to form collaborative networks, HIDS and mobile nodes in the networks are free to move and choose whom to collaborate with. An effective trust management system reduces the negative impact of low expertise HIDSes. There are two types of requests: intrusion consultation messages and test messages. These messages are passed among HIDSes through the communication overlay as shown in the architecture design.

A. Intrusion Consultation

When HIDS detects misbehaviour nodes it has no experience to make decision about the trustworthiness and whether to raise alarm or not. It sends requests to its acquainted HIDSes for consultation in the form of intrusion consultation. Acquaintance management in the trust management processes that requests and sends aggregated feedback and the final destination is made on aggregated results on comparing the trust levels the alarms are raised.

B. Test Messages

The CIDS utilizes the test messages to assess the reliability of one another hubs in the system.

C. Resource Management

The asset the board in the design chooses whether a host IDS ought to apportion assets to react to an interview demand. On assigning assets amid task stage will helps in a few cases, for example, forestalling refusal of administration assaults propelled by sending countless messages to a focused on HIDS. The asset the executives controls the rate of test messages so as to dodge organize just as hubs over-burdening.

D. Correspondence Overlay

It is the fundamental parts which handles all correspondence with different friends in the community oriented system. Messages going through the correspondence overlay incorporates: test messages, conference solicitations to or from neighbors, and input from or to associate administration.

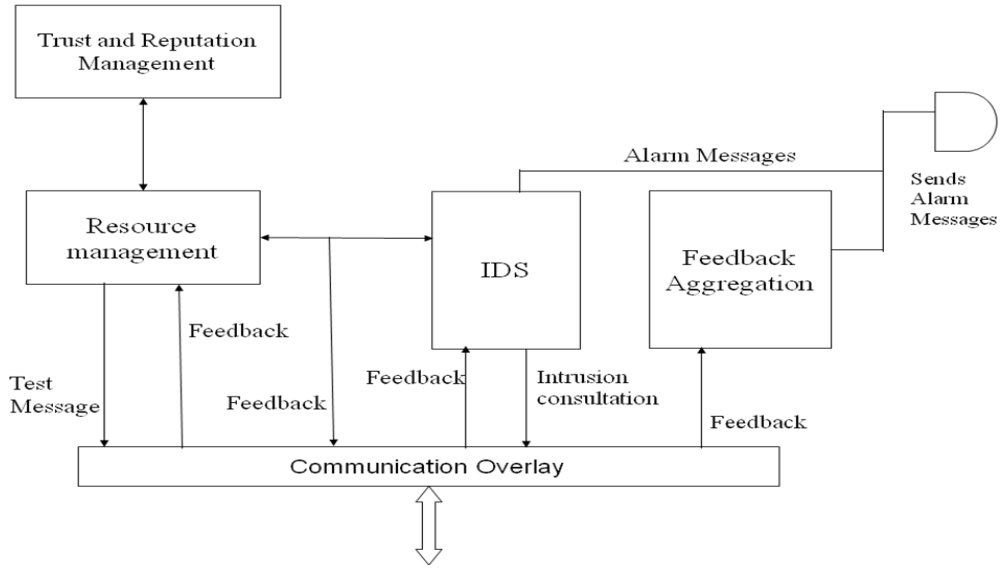

Fig 2: Architecture Diagram

IV. IV. TRUST AND REPUTATION MANAGEMENT

Trust and notoriety the board has as of late turned into a helpful and integral asset in some particular conditions where an absence of past learning about the framework can lead members to undesired circumstances. It gives the dependability to all hubs in the system. Trust and notorieties plans utilized in our venture are Center and Associate executed with neighbour checking calculation.

A. CORE (Collaborative Reputation Mechanism)

CORE is a reputation based generic mechanism for enforcing cooperation of mobile nodes in CRN. CORE is specially designed for CRN to enforce cooperation. CORE stimulates mobile node cooperation by using a collaborative monitoring technique and trust and reputation mechanism. CORE can be integrated with any of the network operations such as, routing and forwarding. In CORE each and every mobile nodes keeps track of other nodes collaboration using a technique called reputation. The nodes are monitored by each of its neighboring nodes, if the behavior of any node changes, the reputation value which is calculated by the monitored neighboring nodes is decreased based on the behavior. And then the overall reputation is calculated based on the collected observations from each nodes, if the reputation value is positive then those nodes are considered as trusted nodes and are therefore be part of the network operations and if the reputation value is negative then the node is considered as un-trusted nodes and latter they are denied from the network operations by punishing them.

The reputation is calculated, formed and updated along time whenever a node requires and also whenever a nodes changes its behavior. In CORE three different types of reputations are used,

1. Subjective Reputation

In subjective reputation, the node calculates the reputation by direct observation of nodes. Subjective reputation gives more relevance to the past observations than the present observation in order to minimize the misbehavior in the recent observations.

2. Indirect Reputation

In indirect reputation, the reputation is calculated from the information provided by the neighboring nodes about the behavior of its monitored nodes. In the collected information, the indirect reputation will considers only the positive values thus by avoiding negative values the common denial of service attacks can be prevented.

3. Functional Reputation

In functional reputation, the reputation values are calculated by combining the features of subjective and indirect reputation with respect to different functions, some of the stated functions are packet forwarding function and routing functions.

B. Components of CORE

1. Network Entity

The network entity of CORE is corresponds to a mobile nodes which are participating in the network. Each entity in a CORE is enriched with a set of Reputation Table (RT) and Watchdog mechanism (WD). The RT and WD combined together constitute the basis of collaborative reputation mechanism. The classification of each entity is based on the performance of each node and has a strong binding between the cooperative behaviors of nodes with resource utilizations. The RT and WD make each node in the network to observe and classify each of its neighbor nodes that gets involved in network operations.

2. Reputation Table

Reputation Table is defined as the data structures which are stored in each node. The row of the table contains the reputation data pertaining to a node and consists of four entries; the unique ID of the node, a collection of recent subjective reputation by direct observation of the node,

a collection of recent indirect reputations provided by the neighboring nodes, and the valued of the calculated reputation with predefined functions.

3. Watchdog Mechanism

The watchdog mechanism in each node is used to monitor its neighboring node and to detect the malicious behavior if any presented in the network. CORE works in promiscuous mode and checks whether all the nodes in the network are performing well. In CORE, watchdog mechanism and reputation table is used for monitoring the nodes and to differentiate trustworthy nodes from untrustworthy nodes in order to improve the performance and throughput of both CORE and network, a profile based neighbor monitoring algorithm is implemented in the components of CORE. Using neighbor monitoring algorithm the selection of false features and excessive features are avoided and improves the performance of CORE in the presence of misbehaving nodes.

C. CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Adhoc NeTworks)

CONFIDANT is a trust and reputation based cooperation enforcement scheme aims to detect selfish behavior and malicious behavior nodes by means of an combined monitoring and reporting mechanisms. The main aim of CONFIDANT is not to allow selfish behavior and misbehavior nodes to destroy the network operations and makes the mobile nodes to cooperate well in network operation by denying misbehavior nodes. In trust and reputation based CONFIDANT protocol the term reputation is used for evaluating the routing and forwarding behavior of the nodes in the network protocol and the term trust is used for evaluating the participation of the mobile nodes in the CONFIDANT protocol. CONFIDANT is implemented in multicast environment where the data packets are transmitted to multiple destinations. It plays an important role in multicast environment by increasing the performance of the routing protocol.

Components of CONFIDANT protocols:CONFIDANT consists of four different components implemented in each node of the network, that includes; **the monitor** (also called as Neighborhood Watch) the nodes of the neighborhood watch will monitors all the neighboring nodes and will detects the deviations of the neighboring nodes. The **trust manager** deals with the incoming and outgoing ALARM messages and the trust manager of a node will send the ALARM messages to all nodes in the network to warn others if the malicious nodes are presented in the network. The **reputation system** is used for handling the first-hand and second-hand information about routing and forwarding behaviors of all the nodes presented in the network. The **path manager** in the nodes will re-rank the path frequently whenever the malicious behavior is detected and it will delete the entire routes containing malicious nodes.

Using profile based neighboring monitoring algorithm the performance of CONFIDANT is improved in detecting malicious nodes and in finding the trusted nodes for network operations.

D. Profile based neighbor monitoring intrusion detection techniques

In profile-based neighboring monitoring schemes each nodes builds a separate profile for each of its neighbors. The features includes in those profiles were, dimension, packet type, flow direction, sampling periods and statistics measures. All were traffic related features; by using those features a node can monitor its neighboring nodes behavior. If the features exceed the threshold, an alert should be raised. Markov blanket discovery is also a feature selection algorithm used in profile based neighbor monitoring algorithm which tries to decrease the number of features selected for network operations without affecting the detection range of IDS. In network more number of trusted nodes was available and all were selected for network operations and all selected features are monitored and profiles are created. By this a large amount of capacity is required for even a small network with very few nodes. In order to overcome this problem a Markov blanket discovery algorithms is applied to select the appropriate features with shortest path.

E. Simulation and Results

The following section describes the simulations results of the proposed system by considering some of the metrics and parameters.

Performance metrics : The following metrics are considered for performance of the networks.

Throughput: The throughput of the network is obtained by the ratio of the number of bits received over the time difference between the first and last received packets.

Packet Delivery Ratio (PDR): The packet delivery ratio of a receiver is defined as the ratio of the number of data packets actually received over the number of data packets transmitted by the senders in the network.

End-to-end Delay: The end-to-end delay of a packet is defined as the time a packet takes to travel from the source to the destination.

V. SIMULATION PARAMETERS AND SIMULATION SETTINGS

The simulation experiment is constructed using Network Simulator version 2.35 (NS 2.35), a scalable and efficient simulation environment for cognitive radio adhoc networks. In the simulated network, 50 mobile nodes are considered as an initial phase and where placed randomly within a 1000 m x 1000 m area. Each node in the network has the transmission range of 250 m and moves with a speed if 1 m/s. In simulation environment, assume each node moves independently with the same constant speed. Also all the nodes in the network have same transmission range of 250 meters.

Table 1: Simulation parameters

Parameters	Value
Number of Nodes	50
Area Size	1000 m x 1000 m
MAC	802.11
Radio Range	250 m
Packet Size (excluding header size)	512 bytes
Mobility Model	Random Way Point
Simulation Time	900 sec
Traffic Source	CBR
Speed	10, 20, 30, 40, 50, 60 m/s
Pause Time	5 sec

The packets speed in the simulation environments is varied from 10 m/s to 60 m/s. The simulated traffic source of the network is Constant Bit Rate (CBR) as shown in Table 1.

A. Simulation results

Figure 3 shows how the trust and reputation based neighbor-monitoring scheme CORE and CONFIDANT implemented in multicast routing protocol handles a varying percentage of malicious nodes in the total mobile adhoc networks. The pause time for the simulation is set to 0 for stressing the CORE and CONFIDANT protocol with a dynamic network to detect the packet dropped ratios in the network. The number of applications running simultaneously in the network is set as high as 30 for the increased load. In a defenseless network like CRN even a very small percentage of malicious nodes may degrade the performance of the network. If the percentage of malicious nodes in the network increases then there will not be much difference in the packet dropping ratio. The fortified network with CORE and CONFIDANT keeps the number of packets dropped low even in the network where malicious nodes are high. The entire routes with malicious behavior are removed from the network and the network even has enough nodes to provide alternate routes during network operations. The ratio of packets dropped is very low in CORE and CONFIDANT implemented networks.

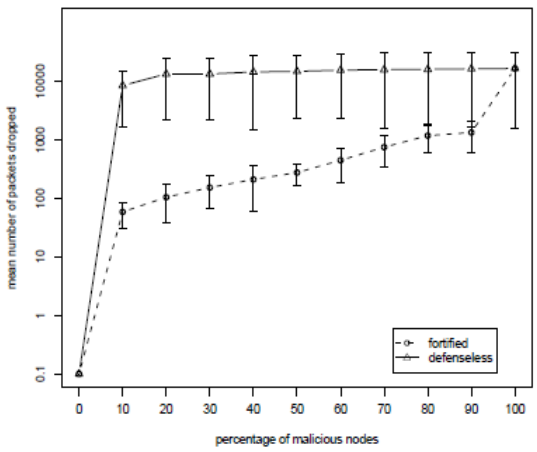

Figure 3: Number of packets dropped with 50 mobile nodes and with varying percentage of malicious nodes.

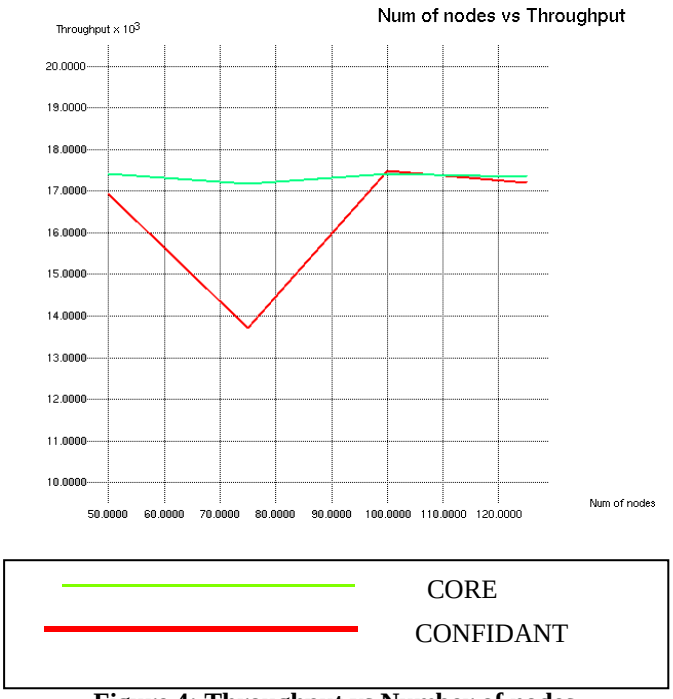

Figure 4: Throughput vs Number of nodes

Figure 4: shows the throughput comparison of CORE AND CONFIDANT according to the CBR application used. The source nodes normally called as clients sends the data packets at a constant bit rate of 2 Mbits and the destination nodes may respond according to the type of data packets they have received. The throughput of the fortified network is very high as shown in the graph it can also take the advantages of longer pause times and makes the performance much higher as compared to other multicast protocols. This shows that our proposed system can identify the misbehavior nodes and punish them accordingly.

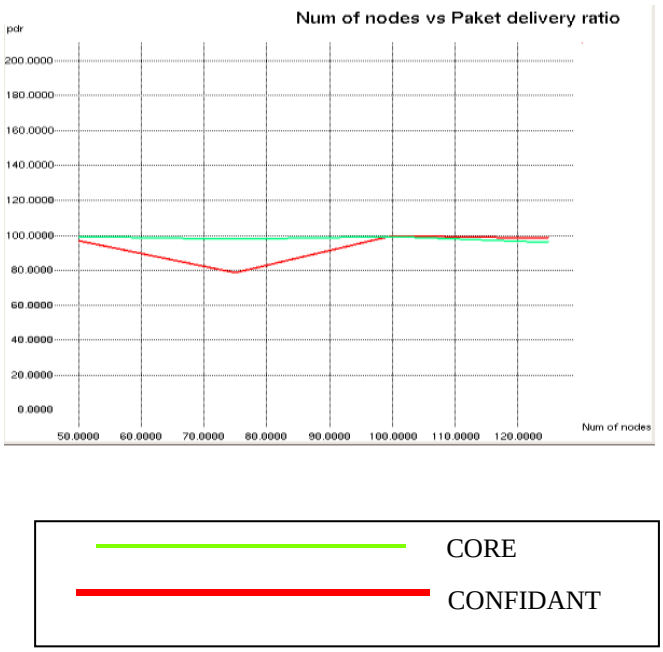

Figure 5: Packet Delivery Ratio vs Number of nodes

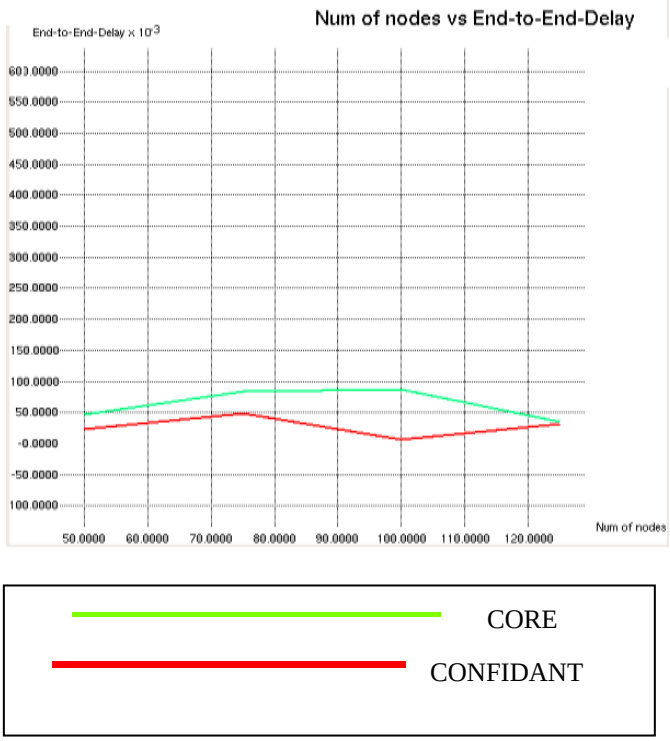

Figure 6: End-to-End Delay vs Number of nodes

Figure 5 and 6 shows the end-to-end delay vs number of nodes of the network with presence of malicious nodes. The end-to-end delay increases if the malicious nodes in the networks are higher. The above figure shows that with neighbor monitoring schemes CORE and CONFIDANT, our proposed system has lower end-to-end delay of the packets.

VI. CONCLUSION AND FUTURE WORK

Trust and reputation management are the most important aspects of mobile adhoc networks. In CRNs achieving trust and reputation management schemes are highly challenging tasks due to the nodes mobility and computation complexity. Nodes will move freely in the network and making the topology of the network changes frequently, by this features of mobile nodes they are more prone to attacks than in wires networks. Countermeasures against the various kinds of attacks and node misbehavior were the main concern in mobile adhoc networks. This research work is focused on CRN where there is lack of trust relationship between the mobile nodes and without trust relationship many nodes are compromised by attackers and the nodes are behaved as malicious nodes.

Trust and reputation management schemes are the fundamental requirements of CRNs. The proposed system gives the comparative study of two trust and reputation schemes (CORE and CONFIDANT) with profile based neighbor monitoring intrusion detection technique, on secured on-demand ODMRP and MAODV routing protocols. CORE is a generic reputation based collaborative mechanism which enforces cooperation of mobile nodes in CRNs and prevents selfish behavior in routing and COFIDANT is a reputation based cooperation schemes aim to detect and isolate misbehaving nodes.

CORE and CONFIDANT are incorporated in routing protocol in order to find trusted nodes during routing process, to increase the performance of routing, the profile based neighbor-monitoring schemes is added in both CORE and CONFIDANT. By this approach the overall network performance is improved and also improves the detection range of finding trusted nodes and detecting malicious nodes. The experimental results show that the proposed trust based collaborative intrusion detection system provides better throughput and packet delivery ratio in multicast routing protocol.

In future, would like to investigate the application of trust and reputation management models and try to implement it in network routing protocols. Further would like to distribute the overall load to all other nodes in the network for balancing the load and would try to investigate the performance of the network. One possible direction for future work is to deploy a real trust based CIDS using the existing IDS in secured routing and use it for the further experimental results.

The main aim is to implement a new trust based algorithm which focuses on both selfish and misbehavior nodes and to neglect the problem of bootstrapping in trust and reputation based system in future.

REFERENCES

1. Manuel Gil Perz, Felix Gomez Marmol, Gregorio Martinex Perez and Antonio F. Skarmeta Gomez. "RepCIDN: A Reputation-based Collaborative Intrusion Detection Network to Lessen the Impact of Malicious Alarms. Journal In Network System Management, Springer. March 2012.
2. P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *The 6th IFIP Conf. on Security Communications, and Multimedia*, Porotoz, Slovenia, 2002.
3. S. Buchegger and J. –Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks," *Proc. 3rd IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing*, Lausanne, CH, 9-11 June 2002, pp. 226-236.
4. Q. He, D. Wu, and P. Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-Hoc Networks," *Proc. IEEE Wireless Communications and Networking Conf.*, vol. 2, pp. 825-830, March 2004.
5. P. G. Argyroudis and D. O'Mahony, "Secure Routing for Mobile Ad Hoc Networks," *IEEE Commun. Surveys and Tutorials*, vol. 7, no. 3, pp. 2-21, 2005.
6. Carol J Fung, Jie Zhang, Issam Aib, Raouf Boutaba. Dirichlet-Based Trust Management for Effective Collaborative Intrusion Detection Networks. In IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 8, NO. 2, JUNE 2011.
7. S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM)*, Boston, 2000.
8. Gomez Marmol, F., Martı´nez Perez, G.: Security threats scenarios in trust and reputation models for distributed systems. Comput. Secur. 28, 545–556 (2009)
9. P. L. Campbell, "The Denial-of-Service Dance," *IEEE Security and Privacy*, vol. 3, no. 6, pp. 34-40, Nov./Dec. 2005.
10. Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security and Privacy*, vol. 2, no. 3, May 2004, pp. 28-39.
11. B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," *Wireless Network Security-Signals and Communication Technology*, Part II, 2007, pp. 103-135, Springer U.S.

12. R. Maheshwari and S. R. Jie Gao Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," *Proc. 26th IEEE Int'l Conf. on Computer Communications*, Anchorage, AK, 6-12 May 2007, pp. 107-115.
13. Boukerche A, Xu L, El-Khatib K. Trust-based security for wirelessad hoc and sensor networks. Computer Communications 2007;30(11–12):2413–27.
14. Haong Lan Nguyen, Uyen Trang Nguyen (2006), "A study of different types of attacks on multicast in mobile ad hoc networks", Department of Computer Science and Engineering, York University, Toronto, Ont., Canada M3J IP3.1570-8705/$.doi:10.1016/j.adhoc.2006.07.005.
15. B. Sun; Y. Guan; J. Chen; U.W. Pooch, Detecting Black-hole Attack in Mobile Ad Hoc Networks[C]; 5thEuropean Personal Mobile Communications Conference, 2003, 490-495.
16. Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *AdHoc Networks Technologies and Protocols (Chapter 9)*, Springer, 2005.
17. P. Michiardi and R. Molva. Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. European Wireless Conference, 2002.
18. M. A. Azer, S. M. El-Kassas, A. W. F. Hassan, M. S. El-Soudani, "A survey on trust and reputation schemes in ad hoc networks," in Third international conference on availability, reliability and security, ARES 08, pp. 881–886, 2008.
19. C. Fung, O. Baysal, J. Zhang, I. Aib, and R. Boutaba, "Trust management for host-based collaborative intrusion detection," in 19th IFIP/IEEE International Workshop Distributed Syst., 2008.
20. J. Douceur, "The sybil attack," in Proc. 1st International Workshop Peer-to-Peer Syst., 2002.
21. Hu, J., Burmester, M., 2006. "LARS: a locally aware reputation system for mobile ad-hoc networks", in 44th annual ACM Southeast Regional Conference.
22. J. H. Cho, A. Swami, and I.R. Chen, "A survey of trust management in mobile ad hoc networks," IEEE Commun. Surveys Tuts., 2011.
23. G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," in The 3rd ACM workshop on Wireless security, WiSe '04, pp. 1–10, 2004.
24. L. Eschenauer, V. D. Gligor, and J. Baras, "On trust establishment in mobile ad-hoc networks," in Security Protocols Workshop, vol. 2845, pp. 47–66, April 2002.
25. P. G. Argyroudis and D. O'Mahony, "Secure Routing for Mobile Ad Hoc Networks," *IEEE Commun. Surveys and Tutorials*, vol. 7, no. 3, pp. 2-21, 2005.
26. N.Shanthi, Dr.Lganesan and Dr.K.Ramar , "Study of Different Attacks on Multicast Mobile Ad hoc Network," Journal of Theoretical and Applied Information Technology.

AUTHORS PROFILE

S. Sankar Ganesh is having teaching experience about 9 years.. He served in various positions in Teaching. He is currently doing as Research Scholar, Department of Computer Science and Engineering, Vinayaka Mission's Research Foundation, Salem, Tamil Nadu, India. His area of interest includes Network Security.

Dr.K.Somasundaram is having industry and teaching experience about 24 years. He served in various positions in industry and Teaching. He is currently serving as Professor and Program Director (Engineering Research) in Computer Science and Engineering department at Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation, Chennai. He published about 80 papers in International journals and presented 32 papers in refereed national & International Conferences. There are 8 scholars are completed their research under his guidance and 8 PhD scholars are doing their research. He guided more than 23 M.E., Thesis. He is a member of IE(India), IETE,CSI, ISTE and CEng(IEI). His area of interest includes Data Mining and Data Analytics, Wireless Sensor Networks, Grid/Cloud computing.