International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

Intrusion Detection Systems in Mobile Ad Hoc Networks: A Review

B.Venkatesh[#1], V.Suresh[*2], A.Anjaneyulu[#3]

[#] *Department of Computer Science and Engineering, JNTU Kakinada University*
[*] *Department of Computer Science and Engineering, JNTU Kakinada University*
Vignan's Institute of Information Technology, Duvvada, Visakhapatnam-530049, India
[1]venky.bandaru@gmail.com , venkatesh.b@vignanvizag.com
[2]vayasisuresh@gmail.com , [3]anjaneyuluala@gmail.com

Abstract— **Mobile ad hoc networks (MANETs) consist of mobile nodes arranged in a manner to collect information about surrounding environment. Their distributed nature, multi-hop data forwarding, and open wireless medium are the factors that make MANETs highly exposed to security attacks at various levels. Intrusion Detection Systems (IDSs) can play an important role in detecting and preventing security attacks. This paper presents current Intrusion Detection Systems and some open research problems related to MANET security.**

Index Terms— Mobile Ad Hoc Network (MANET), Security, Attacks on MANET. (*key words)***

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-arranging network which is formed automatically by a collection of mobile nodes without the help of a fixed structure. Each node is prepared with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the movement of mobile nodes as they move within, move into, or move out of the network. A MANET with the characteristics described above was originally developed for military purposes, as nodes are distributed across a battled and there is no infrastructure to help them form a network. In recent years, MANETs have been developing rapidly and are increasingly being used in many applications, ranging from military to civilian and commercial uses, since setting up such networks can be done without the help of any infrastructure or interaction with a human. Some examples are: search-and-rescue missions, data collection, and virtual classrooms and conferences where laptops, PDA or other mobile devices share wireless medium and communicate to each other. As MANETs become widely used, the security issue has become one of the primary concerns. For example, most of the direction-finding protocols proposed for MANETs assume that every node in the network is cooperative. Therefore, only one compromised node can cause the failure of the entire network.

There are both passive and active attacks in MANETs. For passive attacks, packets containing secret information might be monitored, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication were first brought into consideration, and many techniques have been proposed and implemented. However, these applications are not sufficient. If we have the ability to detect the attack once it comes into the network, we can stop it from doing any damage to the system or any data. Here is where the intrusion detection system comes in.

Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system. The mechanism by which this is achieved is called an intrusion detection system (IDS). An

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once an IDS determines that an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also begin a proper response to the malicious activity. There are several intrusion detection techniques developed for wired networks today, they are not suitable for wireless networks due to the differences in their characteristics. Therefore, those techniques must be modified or new techniques must be developed to make intrusion detection system effectively in MANET's.

II. Important Parameters in MANET Security

Because of MANET's special characteristics, there are some important rules in MANET's security that are important in all security approaches; we call them "Security Parameters". Being unaware of these parameters may cause a security approach useless in MANET.

Figure1 shows the relation between security parameters and security challenges. Each security approach must be aware of security parameters as shown in Figure 1. All mechanisms proposed for security aspects, must be aware of these parameters and don't ignore them, otherwise they may be useless in MANET. Security parameters in MANET are as follow

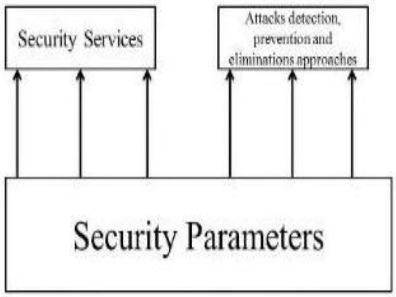

Figure 1. Relation between Security Parameters and Security aspects

Network Overhead:

Network overhead refers to number of control packets generated by security approaches. Due to shared wireless media, additional control packets may easily lead to collision in MANET. Packet lost is one the results of collision.

Therefore, high packet overhead increases packet lost and the number of retransmitted packets. This will easily wastes node's energy and network's resources.

Processing Time:

Each security approach needs time to detect misbehaviors and eliminate malicious nodes. Due to MANET's active topology it's strongly possible that routes between two different nodes break because of mobility. Therefore, security approaches must have low possible processing time in order to increase MANET flexibility and avoid rerouting process.

Energy Consumption:

In MANET nodes have limited energy supply. Therefore, optimizing energy consumption is highly challengeable in MANET. High energy consumption reduces nodes and network's lifetime.

Each security protocol must follow these three important parameters.

MANET Security Challenges

One of the earliest researches in security in MANET was presented in 2002. Generally there are two important aspects in security: Security services and Attacks. Services refer to some protecting policies in order to make a secure network, while attacks use network lifetime to defeat a security service.

Security Services

The aim of a security service is to secure network before any attack happened and made it harder for a malicious node to breaks the security of the network. Due to special features of MANET, these services faced lots of challenges. For securing MANET some services must be provided, which means if one service guarantees without noticing other services, security system will fail. Providing an exchange between these security services is depended on network application, but the problem is to provide services one by one in MANET and presenting a way to guarantee each service.

Availability:

According to this service, each authorized node must have access to all data and services in the network. Availability challenge will come into consideration because of MANET's dynamic topology and open boundary. There is one parameter i.e., accessing time, which is the time needed for a node to access the network services or data is important, because time is one of the security parameters. Authors are provided a new way to solve this problem by using a new approach called clustering approach. In the proposed approach which is called ABTMC (Availability Based Trust Model of Clusters), by using availability based trust model, violent nodes are identified quickly and should be isolated

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

from the network in a period of time, therefore availability of MANET's will be guaranteed.

Authentication:

The aim of this service is to provide trusted communications between two different nodes. When a node receives packets from a source, it must be sure about identity of the source node. One way to provide this service is using certifications, in absence of central control unit. Here key distribution and key management is challengeable. In the above service, authors presented a new way based on trust model and clustering to public the certificate keys. In this case, the network is divided into some clusters and in this clusters public key distribution will be safe by mechanisms. Simulation results show that, the presented approach is better than PGP. But it has some limitations like clustering. MANET dynamic topology and irregular nodes position, made clustering challengeable.

Data confidentially:

According to this service, each node or application must access to specified services that it has the permission to access. Most of services that are provided by data confidentially use encryption methods. But in MANET as there is no central management, key distribution faced lots of challenges and in some cases it is impossible. Authors proposed a new scheme for reliable data delivery to enhance the data confidentially. The basic idea is to transform a secret message into multiple shares by secret sharing schemes and then deliver the shares via multiple independent paths to the destination. Therefore, even if a small number of nodes that are used to transmit the message shares have been compromised, but the secret message as a whole is not compromised. Using multipath delivering causes the variation of delay in packet delivery for different packets. It also leads to out-of-order packet delivery.

Integrity:

According to integrity security service, just authorized nodes can create, edit or delete packets. As an example, Man-In-The-Middle attack is against this service. In this attack, the attacker captures all packets and then removes or modifies them. Authors presented this mechanism to modify the DSR routing protocol and gain to data integrity by securing the discovering phase of routing protocol.

Non-Repudiation:

By using this service, neither source nor destination can reject their behavior or data. In other words, if a node1 receives a packet from node 2, and sends a reply, node 2 cannot reject the packet that it has been sent. Authors presented a new approach that is based on grouping and limiting hops in broadcast packets. All group members have a private key to ensure that another node couldn't create packets with its properties. Detecting and eliminating malicious nodes, is another aspect of the MANET security. Attacks Due to special features like hop-by-hop communications, wireless media, open border and easy to setup, MANET became popular for malicious nodes.

Some of the most important attacks in MANET are as follows:

Black Hole Attack:

In this attack, malicious node injects fault routing information to the network and leads packets toward itself, then rejects all of them.. In this approach, whenever a source node receives RREP packets, it send a confirmation packet through the second best path to the destination and ask the destination whether it has a route to the RREP generator or to the Next-Hop-Node of RREP generator or not. If the destination has no route to this node, both RREP generator and its Next-Hop-Node will mark as malicious nodes. Using this approach source node can detect cooperative malicious node. In the case of more than two cooperative malicious nodes, this approach can't detect all malicious nodes.

Worm Hole Attack:

In worm-hole attack, malicious node records packets at one location of the network and deviate them to another location. Fault routing information could disrupt routes in network. Author presented a way to secure MANET against this attack by using encryption and node location information.

Byzantine attack:

In this attack, malicious node injects fault routing information to the network, in order to locate packets into a loop. One way to protect network against this attack is using authentication. Author presented a mechanism to defeat against this attack using RSA authentication.

Snooping attack:

The goal of this attack is accessing to other nodes packets without permission. As in MANET packets transmitted hop by hop, any malicious node can capture others packets.

Routing attack:

In this attack, malicious node tries to modify or delete node's

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

routing table. Using this attack, malicious node destroys routing information table in ordinal nodes. Therefore, packet overhead and processing time will increase.

Resource consumption attack:

In this attack, malicious node uses some ways to waste nodes or network resources. For instance, malicious node leads packets to a loop that consists of ordinal nodes. As a result, node's energy was consumed for transmitting fault packets. In addition, blocking and packet lost probability will increase.

Session hijacking:

Session hijacking is a critical error and gives an opportunity to the malicious node to behave as a valid system. Using this attack, malicious node reacts instead of true node in communications. Cryptography is one of the most efficient ways to defeat this attack.

Denial of service:

In this attack, malicious node prevents other authorized nodes to access network data or services. Using this attack, a specific node or service will be hard to find and network resources like bandwidth will be wasted. In addition, packet delay and blocking increases.

Jamming attack:

Jamming attack is a kind of DOS attack. The objective of a jammer is to interfere with valid wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of valid packets.

Impersonation Attack:

Using this attack, attacker can pretend itself as another node and injects fault information to the network. As MANET has open border and hop-by-hop communications, it's hardly susceptible against this attack. In some cases using authentication is useless.

Modification Attack:

In this attack, malicious nodes spread the network for a period of time. Then, explore wireless frequency and use it to modify packets. Man-in-the-middle is a kind of Modification attack.

Fabrication Attack:

In fabrication attack, malicious node destroys routing table of nodes by injecting fault information. Malicious node creates fault routing paths. As a result, nodes send their packets in fault routes. Therefore, network resources wasted, packet delivery rate decreased and packet lost will growth.

Man-in-the-middle attack:

In this attack, malicious node puts itself between source and destination. Then, captures all packets and drops or modifies them. Hop by hop communications are made MANET vulnerable against this attack. Authentication and cryptography are the most effective ways to defeat this attack.

Gray Hole Attack:

This attack is similar to black hole. In black hole, malicious node drops all packets, while in this attack, malicious node drops packets with different probabilities. As it relays some packets, detecting this attack is more complicated than black hole and some detection approaches like sniffing or watchdog will be useless in it.

III. Intrusion Detection Systems

One of the key features of a MANET is its multi-hop distributed operations, which add more complexity in terms of security attack detection and prevention. In a multi-hop distributed system, it is very difficult to locate attackers or malicious nodes. Many security attack detection and prevention mechanisms are designed for MANETs; however most of the existing solutions are capable of handling only a few security attacks. For example, most secure routing protocols are designed to counter few security attacks. Similarly new media access mechanisms are designed to handle hidden-node problem. Encryption mechanisms are designed to protect data against passive attacks. Hence, one can say that there is a need to design mechanisms that are capable of detecting and preventing multiple security attacks in MANETs. An Intrusion Detection System (IDS) is one possible solution to it. An intrusion is basically any sort of unlawful activity which is carried out by attackers to harm network resources or sensor nodes. The primary functions of IDS are to monitor user's activities and network behavior at different layers. A single perfect defense is neither possible nor impossible in wireless networks, as there always exist some architectural weaknesses, software bugs, or design flaws which may be compromised by intruders. The best practice to secure wireless networks is to implement multi lines of security mechanisms; that is why IDS is more critical in wireless networks. It is viewed as a passive defense, as it is not proposed to prevent attacks; instead it alerts network

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

administrators about possible attacks well in time to stop or reduce the impact of the attack. The accuracy of intrusion detection is generally measured in terms of false positives (false alarms) and false negatives (attacks not detected). There are two important classes of IDSs. One is known as signature-based IDS, where the signatures of different security attacks are maintained in a database. This kind of IDS is effective against well-known security attacks. However, new attacks are difficult to be detected as their signatures would not be present in the database. The second type is anomaly-based IDS. This kind is effective to detect new attacks; however it sometimes misses to detect well-known security attacks. The reason is that anomaly-based IDSs do not maintain any database, but they continuously monitor traffic patterns or system activities. IDS can operate in two modes, for example, stand-alone operation and cooperative cluster based operation. A standalone IDS operates on every node to detect unwanted activities. Cooperative cluster based IDS are mostly distributed in nature in which every node monitors its neighbors and surrounding nodes activities and operation; in case of any malicious activity detection, the cluster head is informed. IDS has three main components as shown in Figure 2. They are (i) monitoring component (ii) analysis and detection module (iii) alarm

(i)Monitoring component is used for local events monitoring as well as neighbors monitoring. This component mostly monitors traffic patterns, internal events, and resource utilization.

(ii)Analysis and detection module is the main component which is based on modeling algorithm. Network operations, behavior, and activities are analyzed, and decisions are made to declare them as malicious or not.

(iii)Alarm component is a response generating component, which generates an alarm in case of detection of an intrusion.

IDSs are passive in nature and can only detect intrusion. They cannot take any preventive action; they only generate an alarm. It is then the administrator's job to take preventive measures against the attack. Researchers in MANETs are working on two broad categories of IDSs, that is, signature-based and anomaly-based IDSs.

Monitoring Component
Analysis and detection
Alarm

Figure 2: *Components of IDS*

A. Signature-Based Intrusion Detection Systems

Signature-based IDS, also known as rule-based IDS. It has predefined rules of different security attacks. When the network's behavior shows any deviation from the predefined rules, it is classified as an attack. Signature-based IDSs are well suited for known intrusions; however they cannot detect new security attacks. In this section, we present existing signature-based IDSs for MANETs. It is host based in which every node has IDS. The architecture of the proposed IDS has many modules such as packet monitoring, cooperative engine, detection engine, and response unit. The IDS is basically designed for routing attacks and is capable of detecting packet-dropping attacks. The proposed IDS is hosted on each sensor node and requires Tiny OS with the combination of Mint Route routing protocol. It is an advanced version with narrow approach; that is, the former can detect many packet-dropping and misdirecting attacks while the latter is only designed for detection of sink-hole attacks. In both approaches, every node monitors and cooperates with neighbors. Intrusion Detection Program (IDP) is proposed, which is capable to detect known attacks. IDP is based on genetic programming (GP) technique and is effective against a variety of attacks such as denial of service (DoS) and unauthorized access. IDA uses three variants of GP such as linear-genetic programming (LGP), multi-expression programming (MEP), and gene-expression programming (GEP). GEP and MEP detection and classification accuracy are greater than 95%. It uses few fuzzy rule-based classifiers to identify intrusions. The authors claim that fuzzy classifier provides 100% accuracy for all kinds of intrusions.

A decentralized rule-based IDS has three main phases, namely, data acquisition, rule application, and intrusion

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

detection. The proposed mechanism is capable of detecting many routing attacks such as worm-hole, black-hole, selective-forwarding, and delay attacks. The authors also claim that the proposed solution is capable of detecting jamming attack as well; however they did not explain how jamming attacks are detected as it is a physical layer attack. Spontaneous watchdog IDS architecture consists of local and global agents; however it is not implemented yet. An ant-colony-based IDS in conjunction with machine learning is another rule-based IDS. The proposed IDS distinguish behavior and acts using self-organizing principle initiated with probability values. Different signature-based IDSs are given in Table 1.

IDS	Mechanism	Attacks	Evaluation metrics
[25]	Collaborative	Black hole, selective forwarding	Window length, false negative rates
[26]	Local and cooperative detection	Sink hole	Detection rate, false negative rates
[27]	Hierarchical	N/A	N/A
[28]	Genetic programming	DoS, unauthorized access	Classification accuracy
[29]	Soft computing	Unauthorized access, probing	Classification accuracy
[30]	Specification based	Repetition attack, delay attack, worm hole, alteration attack, black hole, selective forwarding	Detection rate, false positives
[31]	Spontaneous watchdog	N/A	N/A
[32]	Ant colony	Abnormal transmission	N/A

Table 1: *Signature based IDSs.*

B. Anomaly-Based Intrusion Detection Systems

Anomaly-based IDS monitors network activities and classifies them as either normal or malicious using heuristic approach. Most of anomaly-based IDSs identify intrusions using threshold values; that is, any activity below a threshold is normal, while any condition above a threshold is classified as an intrusion. The main advantage of anomaly-based IDS is its capability to detect new and unknown attacks; however sometimes it fails to detect even well-known security attacks. Many anomaly-based IDSs have been proposed so far. An unsupervised neural network based IDS is capable of learning and detecting unknown attacks. This intelligent system learns the time-related changes using Markov model. When any intrusion occurs, a mobile agent moves to the malicious region of the WSN to investigate. The proposed mechanism can detect time-related changes and events. A set of intrusion detection techniques are independent of each other. At physical layer, RSSI values are used to detect masquerade, while at network layer, a specialized table driven routing protocol is used to detect routing and authentication attacks. A cluster based IDS for routing attack is capable of building a normal traffic model, which is used to differentiate between normal and abnormal traffic. The normal traffic model consists of number of packets received and sent, number of route requests received and sent, and so forth. The IDS can detect many attacks such as periodic route error attack and sink-hole attack. A support vector machine based IDS is used to detect routing attacks such as black hole. It is basically cooperation based detection in which nodes communicates and share information about security attacks. A cross feature based anomaly detection mechanism monitors and learns normal traffic patterns in order to detect any intrusion in case of deviation. The IDS is capable of detecting packet-dropping and misdirecting attacks. A sliding window based IDS using threshold value is efficient in the detection of few security attacks such as route depletion attacks. Table 2 presents a summary of a number of anomaly-based IDSs.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

IDS	Mechanism	Attacks
[34]	Artificial neural network	Time related changes
[35]	Set of techniques at OSI layers	Masquerade, routing attacks
[36]	Cluster based	Periodic route error attack, sink hole attack
[37]	Support vector	Black-hole attacks
[38]	Cross feature	Packet dropping attacks
[39]	Sliding window	Route depletion attack

Table 2: *Anomaly based IDSs.*

C. Hybrid Intrusion Detection Systems

Hybrid IDSs are a combination of both anomaly-based and signature-based approaches. Hybrid mechanisms usually contain two detection modules; that is, one module is responsible of detecting well-known attacks using signatures, while the other is responsible for detecting and learning normal and malicious patterns or monitor network behavior deviation from normal profile. Hybrid IDSs are more accurate in terms of attack detection with less number of false positives. However, such mechanisms consume more energy and more resources. Hybrid IDSs are generally not recommended for a resource constraint networks such as a WSN; however they are still an active research area. In a hybrid intrusion detection model sensor nodes are divided into hexagonal regions like cellular networks. Each region is monitored by a cluster node, while cluster nodes are monitored by regional nodes. The base station has the responsibility to monitor all regional nodes. It is hierarchical in nature forming a tree-like structure. Attack signatures are stored in base station and propagated toward the leaf node for attack detection. Similarly the mechanism has predefined specifications of normal and abnormal behavior. Anomaly detection is done by measuring deviation from defined specifications. The authors did not mention detection rate or false-alarm ratio of their proposed mechanism. Furthermore, it is not clear which security attacks are detected using this mechanism.

Another hybrid IDS using support vector machine (SVM) and misuse detection is introduced. A distributed learning algorithm is used to train SVM to distinguish normal and malicious patterns. This intrusion detection mechanism is designed to operate in cluster based WSNs, where all nodes monitor their neighbors. The authors claim high detection rate with fewer false positives; however attack types are not described. An IDS that uses state transition analysis and stream slow to detect sync-flood attack against WSNs mechanism monitors three-way handshake of TCP to identify attack pattern; however it is not yet implemented and tested. For a cluster based hybrid IDS, the cluster head is responsible for detecting intrusions. The key idea behind this mechanism is to reduce energy consumption. The enhanced IDS has three modules, that is, anomaly-based detection, signature-based detection, and decision making. A supervised back propagation network is used to learn and identify normal and malicious packets. Another hierarchical hybrid IDS for detection of routing attacks has high accuracy in terms of detection of network layer security attacks such as sink hole and worm hole. Table 3 presents a summary of a few hybrid IDSs.

IDS	Mechanism	Attacks
[40]	Hybrid, hierarchical	N/A
[41]	Support vector machine	N/A
[42]	State transition	Sync flood
[43]	Cluster based	Routing attacks
[44]	Cluster based, supervised learning, misuse detection	Routing attacks
[45]	Hierarchical and hybrid	Sink hole, worm hole

Table 3: *Hybrid IDSs.*

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

D. Cross Layer Intrusion Detection Systems

Cross layer design is a relatively new security technique in which different parameters across OSI layers are exchanged for optimal solutions. Traditional IDS operates at a single layer of the OSI model and hence can monitor and detect intrusions at that particular layer. For example, network layer Intrusion Detection System can detect only routing attacks but cannot respond to MAC, physical, or transport layer anomalies. Cross layer IDSs have the capability to monitor and detect intrusions at multiple layers by communicating and exchanging parameters amongst different layers using cross layer interface. As we know, WSNs have many constraints in terms of computations, memory, and energy. Although cross layer IDS can detect many intrusions at different layers, this technique consumes more energy and computational resources by monitoring, analyzing, and exchanging multilayer parameters. Cross layer intrusion detection agent (CLIDA) for WSNs ensures cross layer information exchange amongst physical, MAC, and network layer. Cross layer data module collects and represents data to all layers. CLIDA is capable of detecting multi-layer security attacks. This architecture has good detection rate; however energy and computational comparison is not given, which could be more interesting. Another cross layer security mechanism for MANET would exhaust the limited resources of sensor nodes. A real-time cross layer security mechanism for large scale flood detection and attack trace-back mechanism uses different parameters from MAC and network layers to detect multi-layer flooding attacks. It maintains different profiles for low, medium, and high intensity attacks.

E. Comparison and Discussion

Mobile Ad Hoc Networks are distributed in nature using the multi-hop communication model. These networks are usually deployed in such areas where direct human interaction is either impossible or very difficult. Furthermore, MANETs have limitations in terms of computation, bandwidth, memory, and energy. These limitations are considered while designing any proposal for such networks. Due to the hostile environments of MANETs, security is one of their most important aspects. IDSs are widely used for securing MANTEs. IDS has the ability to detect an intrusion and raise an alarm for appropriate action. Due to the energy and computational power limitations, designing appropriate IDS for MANETs is a challenging task.

Anomaly-based IDSs are suitable for small-sized MANETs where few nodes communicate with the base station. In small sized MANETs, the traffic pattern is mostly the same, so unusual traffic pattern or changing behaviour can be treated as an intrusion. However such IDS may generate more false alarms and may not be able to detect well-known intrusions. Anomaly-based IDSs are usually lightweight in nature and mostly use statistical, probabilistic, traffic analysis or intelligent techniques.

Signature-based IDSs are suitable for relatively large-sized MANETs, where more security threats and attacks can compromise network operations. Signature-based IDS needs more resources and computations as compared to anomaly-based IDS. One of the important and complex activities is the compilation and insertion of new attack signatures in the databases. Such IDSs mostly use data mining or pattern matching techniques.

Hybrid IDSs are suitable for large and sustainable MANETs. These IDSs have both anomaly-based and signature-based modules, so they require more resources and computations. To reduce the usage of limited resources, such mechanisms are mostly used in cluster based or hierarchical MANETs, in which some parts of the network are used to execute anomaly detection while other parts are accompanied with signature-based detection.

Cross layer IDSs are usually not recommended for a resource constraint networks such as MANETs, as it consumes more resources by exchanging parameters across the protocol suits for attack detection. Table 4 gives the comparison and characteristics of different IDSs.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

Characteristics	Anomaly based IDS	Signature based IDS	Hybrid IDS	Cross layer IDS
Detection rate	Medium	Medium	High	High
False alarm	Medium	Medium	Low	Low
Computation	Low	Low	Medium	High
Energy consumption	Low	Low	Medium	High
Attack detection	Few	Few	More	More
Multilayer attack detections	No	No	No	Yes
Strength	Capable of detecting new attacks	Detects all those attacks having signatures	Can detect both existing and new attacks	Can detect multilayer attacks
Weakness	Misses well known attack	Cannot detect new attacks	Requires more computation and resources	Requires more resources
Suitable for WSN	Yes	Yes	With justification	With strong justification

Table 4: *Comparison of different IDSs*

CONCLUSIONS

While designing a security mechanism, we must consider the limited resources of MANETs. Anomaly-based IDSs are lightweight in nature; however they create more false alarms. Signature-based IDSs are suitable for relatively large-sized MANETs; however they have some overheads such as updating and inserting new signatures. Cross layer IDSs are usually not recommended for networks having resources limitations, as more energy and computation are required for exchanging multilayer parameters.

REFERENCES

[1] Y. Zhang, W. Lee, and Y. Huang, Intrusion Detection Techniques for Mobile Wireless Networks," *ACM/Kluwer Wireless Networks Journal (ACM WINET)*, Vol. 9, No. 5, September 2003.

[2] M. G. Zapata, \Secure Ad Hoc On-Demand Distance Vector (SAODV)Routing," *ACM Mobile Computing and Communication Review(MC2R)*, Vol. 6, No. 3, pp. 106-107, July 2002.

[3] Y. Hu, D. B. Johnson, and A. Perrig, \SEAD: Secure E±cient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), pp. 3-13, June 2002.

[4] Y. Hu, A. Perrig, and D. B. Johnson, \Ariadne: A secure On Demand Routing Protocol for Ad hoc Networks," *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02)*, pp. 12-23, September
2002.

[5] A. Perrig, R. Canetti, D. Tygar and D. Song, \The TESLA Broadcast Authentication Protocol, "*RSA CryptoBytes*, 5 (summer), 2002.

[6]S. Khan, K. K. Loo, and Z. U. Din, "Framework for intrusion detection in IEEE 802.11 wireless mesh networks," *International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 435–440, 2010. View at Google Scholar · View at Scopus

[7] R.Sheikh, M. S. Chande, and D. K. Mishra, "Security issues in MANET:A review," presented at the Seventh International Conference On Wireless And Optical Communications Networks (WOCN), 2010.

[8] H.Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, 2002.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

[9] H.Nishiyama, T. Ngo, N. Ansari, and N. Kato, "On Minimizing the Impact of Mobility on Topology Control in Mobile Ad Hoc Networks," Wireless Communications, IEEE Transactions, 2012.

[10] Y.Z.a and W. Lee, "Intrusion Detection in Wireless Ad Hoc networks," presented at the 6th Int'l. Conf. Mobile Comp. Net., MobiCom, 2000.

[11] F.S.a and R. Anderson, "The Resurrecting Ducking: Security Issues for Ad-Hoc Wireless Networks," 7th Int'l. Wksp on Security Protocols. Proc., LNC, 1999.

[12] X.Zhao, Z. You, Z. Zhao, D. Chen, and F. Peng, "Availability Based Trust Model of Clusters for MANET," presented at the 7th International Conference on Service Systems and Service Management (ICSSSM), 2011.

[13] E.C.H.Ngai and L. M. R, "Trust and clustering-based Authentication Services in Mobile ad hoc networks," presented at the proceeding of the 24th international conference on Distributed Computing systems Workshops 2004.

[14] W.Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," presented at the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, 2004.

[15] S.Rana and A. Kapil, "Security-Aware Efficient Route Discovery for DSR in MANET," Information and Communication Technologies, Communications in Computer and Information Science, vol. 101, pp. 186-194, 2010.

[16] X.Lv and H. Li, "Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks," Information Security, IET, vol. 7, 2013.

[17] S.a.A.k.G, H.o.d.R.m, and S. Sharma, "A Comprehensive Review of Security Issues in Manets," International Journal of Computer Applications vol. 69 2013.

[18] V.P and R.P.Goyal, "MANET: Vulnerabilities, Challenges, Attacks, Application," IJCEM International journal of Computational Engineering & management, vol. 11, 2011.

[19] A.MISHRA, R. Jaiswal, and S. Sharma, "A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network," presented at the 3rd International Conference on Advance Computing Conference (IACC), 2013

[20] A.dorri and T. m. k. zade, "ذآی و یپهاراهی هتلح ل کش," presented at the first regional computing in electronics and engineering, 2014.

[21] N.-W. Lo and F.-L. Liu, "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET," in Intelligent Technologies and Engineering Systems. vol. 234, J. Juang and Y.-C. Huang, Eds., ed: Springer New York, 2013, pp. 59-65.

[22] M.A. Gorlatova, P. C. Mason, M. Wang, and L. Lamont, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," Military Communications Conference, IEEE, MILCOM, 2006.

[23] S.Keer and A. Suryavanshi, "To prevent wormhole attacks using wireless protocol in MANET," presented at the International Conference on Computer and Communication Technology (ICCCT), 2010.

[24] Z.A.Khan and M. H. Islam, "Wormhole attack: A new detection technique," presented at the international conference on Emerging Technologies (ICET), 2012.

[25] M.Yu, M. C. Zhou, and W. Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments," IEEE

Transactions on Vehicular Technology, vol. 58

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

[26] G.Singla, M. S. Sathisha, A. Ranjan, S. D., and P. Kumara, "Implementation of protected routing to defend byzantine attacks for MANET's," International Journal of Advanced Research in Computer Science, vol. 3, p. 109, 2012.

[27] G.Singla and P. Kaliyar, "A Secure Routing Protocol for MANETs Against Byzantine Attacks," Computer Networks & Communications (NetCom), Lecture Notes in Electrical Engineering, vol. 131, pp. 571-578, 2013.

[28] S.Shaw, K. Orea, P. Venkateswaran, and R. Nandi, " Simulation and Performance Analysis of OLSR under Identity Spoofing Attack for Mobile Ad-Hoc Networks," Computer Networks and Information Technologies Communications in Computer and Information Science, vol. 142, pp. 308-310, 2011.

[29] B.Kannhavong, H. Nakayama, Y. Nemoto, and N. Kato, "A survey of routing attacks in mobile ad hoc networks," Wireless Communications, IEEE Transactions, vol. 14

[30]M.Abdelhaq, R. Hassan, and R. Alsaqour, "Using Dendritic Cell Algorithm to Detect the Resource Consumption Attack over MANET," Software Engineering and Computer Systems Communications in Computer and Information Science vol. 181, pp. 429-442, 2011.

[31] L.Rajeswari, A. Prema, R. A. Xavier, and A. Kannan, "Enhanced intrusion detection techniques for mobile ad hoc networks," presented at the International Conference on Information and Communication Technology in Electrical Sciences (ICTES), 2007.

[32] A.K.Rai, R. R. Tewari, and S. K. Upadhyay, "different type of attacks on integrated MANET- internet comunication," international journal of

computer science and security (IJCSS), vol. 4.

[33] J.Y.Kim, H. K. Choi, and S. Song, "A secure and lightweight approach for routing optimization in mobile IPv6," EURASIP Journal on Wireless Communications and Networking - Special issue on wireless network security, vol. 7, 2009.

[34] Supriya and M. Khari, "Mobile Ad Hoc Netwoks Security Attacks and Secured Routing Protocols: A Survey," Advances in Computer Science and Information Technology. Networks and Communications Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 84, pp. 119-124, 2012.

[35] J.Soryal and T. Saadawi, "IEEE 802.11 Denial of Service attack detection in MANET," Wireless Telecommunications Symposium (WTS), 2012.

[36] R.H.Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS Attacks in Mobile Ad Hoc Networks: A Survey," presented at the Second International Conference on Advanced Computing & Communication Technologies (ACCT), 2012

[37] A.Michael and Nadeem, "Adaptive intrusion detection & prevention of denial of service attacks in MANETs," presented at the IWCMC '09 Proceedings of the International Conference on Wireless Communications and Mobile Computing, Connecting the World Wirelessly, 2009.

[38] J.Su and H. Liu, "Protecting Flow Design for DoS Attack and Defense at the MAC Layer in Mobile Ad Hoc Network," Applied Informatics and Communication Communications in Computer and Information Science, vol. 224, pp. 233-240, 2011.

[39] A.Hamieh and J. Ben-othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution," presented at the International Conference on Communications,

ICC '09. IEEE, 2009.

[40] J.Ben-othman and A. Hamieh, "Defending method against jamming attack in wireless ad hoc networks,"

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

presented at the 34th Conference on Local Computer Networks, LCN, IEEE, 2009.

[41] D.Glynos, P. Kotzanikolaou, and C. Douligeris, "Preventing impersonation attacks in MANET with multi-factor authentication," hird International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, WIOPT, 2005.

[42] C.Douligeris, P. Kotzanikolaou, and D. Glynos, "Preventing Impersonation Attacks in MANET with Multi-Factor Authentication," WIOPT '05 Proceedings of the Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2005.

[43] M.Barbeau, J. Hall, and E. Kranakis, "Detecting Impersonation Attacks in Future Wireless and Mobile Networks," Secure Mobile Ad-hoc Networks and Sensors Lecture Notes in Computer Science, vol. 4074, pp. 80-95, 2006.

[44] N.Dixit, S. Agrawal, and V. K. Singh, "A Proposed Solution for security Issues In MANETs," International Journal of Engineering Research & Technology (IJERT), vol. 2, 2013.

[45] Vaithiyanathan, S. R. Gracelin, E. N. Edna, and S. Radha, "A Novel Method for Detection and Elimination of Modification Attack and TTL Attack in NTP Based Routing Algorithm," presented at the International Conference on Recent Trends in Information, Telecommunication and Computing (ITC), 2010

[46] P.Yi, X. Jiang, and Y. Wu, "Distributed intrusion detection for mobile ad hoc networks," Journal on Systems Engineering and Electronics, IEEE, vol. 19, 2008.

[47] S.R. Afzal, S. Biswas, J. B. Koh, T. Raza, and m. authors, "RSRP: A Robust Secure Routing Protocol for Mobile Ad Hoc Networks," presented at the Wireless Communications and Networking Conference, WCNC, IEEE, 2008.

[48] P.T. Tharani, K. Muthupriya, and C. Timotta, "Secured consistent network for coping up with gabrication attack in MANET," international journal of Emerging Technology and Advanced Engeineering, vol. 3, 2013.

[49] D.Sharma, P. G. Shah, and X. Huang, "Protecting from Attacking the Man-in-Middle in Wireless Sensor Networks with Elliptic Curve Cryptography Key Exchange," presented at the NSS '10 Proceedings of the Fourth International Conference on Network and System Security, 2010.

[50] K.Vishnu, "A new kind of transport layer attack in wireless Ad Hoc Networks," presented at the International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010

[51] X.Zou, A. Thukral, and B. Ramamurthy, "An Authenticated Key Agreement Protocol for Mobile Ad Hoc Networks," Mobile Ad-hoc and Sensor Networks Lecture Notes in Computer Science, vol. 4325, pp. 509-520, 2006.

[52] J.Liu, F. Fu, J. Xiao, and Y. Lu, "Secure Routing for Mobile Ad Hoc Networks," presented at the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, SNPD, 2007.

[53] J.Sen, B. Tata, M. Chandra, S. Harihara, and H. Reddy, "A mechanism for detection of gray hole attack in mobile Ad Hoc networks," presented at the 6th International Conference on Information, Communications & Signal Processing, 2007.

[54] G.Usha and S. Bose, "Impact of Gray hole attack on adhoc networks," presented at the International Conference on Information Communication and Embedded Systems (ICICES), 2013

[55] G.Xiaopeng and C. Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks," presented at the IFIP International Conference on Network and Parallel

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

Computing Workshops, NPC Workshops, 2007.

[56]. S. Khan, N. A. Alrajeh, and K.-K. Loo, "Secure route selection in wireless mesh networks," *Journal of Computer Networks*, vol. 56, no. 2, pp. 491–503, 2012. View at Publisher · View at Google Scholar

[57].D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, 2005. View at Google Scholar

[58].M. S. Siddiqui and S. H. Choong, "Security issues in wireless mesh networks," in *Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE '07)*, pp. 717–722, April 2007. View at Publisher · View at Google Scholar · View at Scopus

[59]. S. Khan and K.-K. Loo, "Real-time cross-layer design for a large-scale ood detection and attack trace-back mechanism in IEEE 802.11 wireless mesh networks," *Network Security*, vol. 2009, no. 5, pp. 9–16, 2009. View at Publisher · View at Google Scholar · View at Scopus

[60].I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in *Proceedings of the 13th European Wireless Conference*, Paris, France, April 2007.

[61].I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of Sinkhole attacks in wireless sensor networks," in *Algorithmic*

Aspects of Wireless Sensor Networks ALGOSENSORS, vol. 4837 of *Lecture Notes in Computer Science*, pp. 150–161, Springer, 2008. View at Publisher · View at Google Scholar · View at Scopus

[62].H.Jadidoleslamy, "A hierarchical intrusion detection architecture for wireless sensor networks,"*International Journal of Network Security & Its Applications*, vol. 3, no. 5, 2011. View at Google Scholar

[63].A. Abraham, C. Grosan, and C. Martin-Vide, "Evolutionary design of intrusion detection programs," *International Journal of Network Security*, vol. 4, no. 3, pp. 328–339, 2007. View at Google Scholar

[65].A. Abraham, R. Jain, J. omas, and S. Y. Han, "D-SCIDS: distributed so computing intrusion detection system," *Journal of Network and Computer Applications*, vol. 30, no. 1, pp. 81–98, 2007. View at Publisher · View at Google Scholar · View at Scopus

[66].A. P. R. Da Silva, A. A. F. Loureiro, M. H. T. Martins, L. B. Ruiz, B. P. S. Rocha, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in *Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05)*, pp. 16–23, Montreal, Canada, October 2005. View at Publisher · View at Google Scholar · View at Scopus

[67]S. Banerjee, C. Grosan, and A. Abraham, "IDEAS: Intrusion detection based on emotional ants for sensors," in *Proceedings of the 5th International Conference on Intelligent Systems Design and Applications (ISDA '05)*, pp. 344–349, September 2005. View at Publisher · View at Google Scholar · View at Scopus

[68]M. S. Islam and S. A. Rahman, "Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches,"

International Journal of Advanced Sciences and Technology, vol. 36, pp. 1–8, 2011. View at Google Scholar

[69]Y. Y. Li and L. E. Parker, "Intruder detection using a wireless sensor network with an intelligent mobile robot response," in *IEEE Conference Southeastcon*, pp. 37–42, April 2008. View at Publisher · View at Google Scholar · View at Scopus

[70]V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *Journal of High Speed Networks*, vol. 15, no. 1, pp. 33–51, 2006. View at Google Scholar ·

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

View at Scopus 35.

[71]C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2, no. 4, pp. 313–332, 2006. View at Publisher · View at Google Scholar · View at Scopus

[72]H. Deng, Q. A. Zeng, and D. P. Agrawal, "SVM-based intrusion detection system for wireless ad hoc networks," in *Proceedings of the 58th IEEE Vehicular Technology Conference (VTC '03)*, pp. 2147–2151, October 2003. View at Scopus

[73]Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in *Proceedings of the 23th IEEE International Conference on Distributed Computing Systems*, pp. 478–487, May 2003. View at Scopus

[74]I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '2005)*, pp. 253–259, August 2005. View at Publisher · View at Google Scholar · View at Scopus

[75]M. S. I. Mamun and A. F. M. Sultanul Kabir, "Hierarchical design based intrusion detection system for wireless ad hoc sensor network," *International Journal of Network Security & Its Applications*, vol. 2, no. 3, 2010. View at Google Scholar

[76]H. Sedjelmaci and M. Feham, "Novel hybrid intrusion detection system for clustered wireless sensor network," *International Journal of Network Security & Its Applications*, vol. 3, no. 4, 2011. View at Google Scholar

[77]R. Bhatnagar and U. Shankar, " e proposal of hybrid intrusion detection for defence of sync ood attack in wireless sensor network," *International Journal of Computer Science & Engineering Survey*, vol. 3, no. 2, pp. 31–38, 2012. View at Publisher · View at Google Scholar

[78]K. Q. Yan, S. C. Wang, and C. W. Liu, "A hybrid intrusion detection system of cluster-based wireless sensor networks," in *Proceedings of the International Multi Conference of Engineers and Computer Scientists (IMECS '09)*, Hong Kong, 2009.

[79] K. Q. Yan, S. C. Wang, S. S. Wang, and C. W. Liu, "Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network," in *Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT '10)*, pp. 114–118, Chengdu, China, July 2010. View at Publisher · View at Google Scholar · View at Scopus

[80]T. H. Hai, F. Khan, and E. N. Huh, "Hybrid intrusion detection system for wireless sensor networks," in *Computational Science and Its Applications—ICCSA 2007*, vol. 4706 of *Lecture Notes in Computer Science*, pp. 383–396, Springer, Berlin, Germany, 2007. View at Google Scholar · View at Scopus

[81]S. Khan, K.-K. Loo, and Z. U. Din, "Cross layer design for routing and security in multi-hop wireless networks," *International Journal of Information Assurance and Security*, vol. 4, no. 2, pp. 170–173, 2009. View at Google Scholar

[82]D. E. Boubiche and A. Bilami, "Cross layer intrusion detection system for wireless sensor network," *International Journal of Network Security & Its Applications*, vol. 4, no. 2, 2012. View at Google Scholar

[83]M. Xiao, X. Wang, and G. Yang, "Cross-layer design for the security of wireless sensor networks," in *Proceedings of the 6th World Congress on Intelligent Control and Automation (WCICA '06)*, pp. 104–108, Dalian, China, June 2006. View at Publisher · View at Google Scholar .View at Scopus

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-117 PAGE NO: 679-693.

AUTHER'S PROFILE

[1]**B.Venkatesh** received his B.Tech Degree in Information Technology from JNTU, Hyderabad, Andhra Pradesh in 2006 and the M.Tech Degree in Computer Science and Engineering from JNTU, Kakinada, and Andhra Pradesh, India in 2013. His specializations are Data Mining, Computer Networks, Network Security and Cryptography, Soft Computing, Cloud Computing and Big Data. Presently, he is an Assistant Professor, ECM Department in Vignan's Institute of Information Technology, Visakhapatnam, and Andhra Pradesh, India. He had 11 years of teaching experience. He is a LIFE Member (LM53957) of ISTE (Indian Society for Technical Education).

[2]**V.Suresh** received his B.E. Degree in Electronics and Communication Engineering from University of Madras in 1998 and the M.Tech Degree in Computer Science and Technology from Andhra University, Andhra Pradesh. India in 2002.He is pursuing Ph.D in Computer Science from Andhra University, Andhra Pradesh. India. His specializations are Network Security and Cryptography, Image Processing and Soft Computing, Big Data. Presently, he is an Assistant Professor, ECM Department in Vignan's Institute of Information Technology, Visakhapatnam, and Andhra Pradesh, India. He had 17 years of teaching and 4 years of Industrial experience. He is a LIFE Member of Computer Society of India(CSI) (00174296), Institute of Electronics and Telecommunications Engineers (IETE) (M155602) and Associate Member in Institute of Engineers (IEI) (AM0915397).

[3]**A.Anjaneyulu** received his B.Tech Degree in Computer Science and Engineering from Andhra University in 2013 and the M.Tech Degree in Computer Science and Technology from Andhra University, Andhra Pradesh. India in 2015. His specializations are Computer Networks, Network Security and Cryptography, Image Processing and Soft Computing. Presently, he is an Assistant Professor, ECM Department in Vignan's Institute of Information Technology, Visakhapatnam, Andhra Pradesh, India.