An Ameliorated Methodology for MANET Security using Artificial Intelligence and Dynamic Cache Segmentation

1Mamatha C M, 2Jagadish P, 3Anjank Koundinya
1Associate Professor, 2Assistant Professor
1Cambridge Institute of Technology North Campus,
2BMS, Institute of Technology and Management, Bengaluru,
3BMS, Institute of Technology and Management, Bengaluru

Abstract - **The paper contains a new concept where Cluster of sensor nodes are secured by Artificial Intelligence (AI), and performance is increased by using dynamic cache segmentation. It explains how AI actually safeguards Cluster of sensor nodes. Though AI is used for many purposes such as Gaming, Robotics etc., it is not yet used for Cluster of sensor nodes. In detail, the paper presents the functioning of AI as a protective layer. It mainly focuses on Data Security and Performance Increase. WSN provides a variety of computing resources, from servers and storage to enterprise applications such as email, security, backup/DR, voice, all delivered over the Internet. It is the intelligence exhibited by machines or software. It is an academic field of study which studies how to create computers and computer software that are capable of intelligent behavior. Recently, dynamic content, whose construction is changed dynamically according to an user's request, has been wide-spreading across the sensor nodes. This paper proposes a technique to fast response to the dynamic content of various sensor nodes by the help of cache segmentation between server and the user, and describes the design and implementation of our proposed network cache system and provides security to cluster nodes by using AI as a barrier where every data files goes inside cluster. It gets scanned by AI for viruses and makes data virus-free.**

keywords - **MARIN, DCS, Cluster, Artificial Intelligence , CSA (Cluster Security Alliance).**

Introduction

Nowadays, Wireless Sensor Networks is the most developing field. Though we have many uses through Clusters which are not secure and more delay in data transfer. Some of the WSN applications are

- Habitat and Ecosystem Monitoring
- Seismic Monitoring
- Civil Structural Health Monitoring,
- Monitoring Groundwater Contamination,
- Rapid Emergency Response
- Industrial Process Monitoring,
- Perimeter Security and Surveillance and
- Automated Building Climate Control.

Since many kinds of dynamic content are served from the origin servers, it is more difficult in general to improve a responsiveness of dynamic content than static one that can be cached at a location close to users.

MARIN with DCS is Cluster nodes Artificial Intelligence with Dynamic Cache Segmentation, software which provides AI (artificial intelligence) Security to Cluster nodes along with Increasing in the dynamic content responsiveness of sensor nodes and life time as well. According to CSA (Cluster security Alliance) there are 9 Security problems that WSN is facing, which is often called as Notorious nine. Those are: Data Breaches & Data Loss. Account Hijacking. Insecure AIP's. Denial of service. Malicious Insiders. Abuse and Nefarious use. Insufficient due diligence. Shared Technology Issue.

Along with above some of the Challenges of WSN are Energy Efficiency • Responsiveness • Robustness • Self-Configuration and Adaptation • Scalability •Heterogeneity • Systematic Design • Privacy and Security

By introducing MARIN with DCS we are solving several issues like, Data Breaches, Data Loss, Account Hijacking, Shared technology Issue, Malicious Insiders, abuse and nefarious use, Energy Efficiency, Responsiveness.

Dynamic content is referred to as web pages whose construction, such as displayed images and processing results is varied in response to users' requests. It is generated at the origin web servers located in the service providers and is then transferred to the users. Static content, whose construction is fixed, can be cached at cache servers located near users and be served locally when the same request comes from other users. The pre-fetching is effective in terms of the responsiveness; there is no benefit of caching due to little reuse probability. On the other hand, the one generated based on queries in users' requests which may be identical among multiple users, and caching such dynamic content is promising to give improved

performance of web services. The WSN delivers a hosting environment that is immediate, flexible, scalable and available – while saving corporations money, time and resources. It provides ondemand access to virtualized IT resources that can share by others. From past few years, WSN is not as secure andsafe as it was earlier. But now, cyber criminals hack data of WSN in an easier way, they transfer malicious virus intothe cluster. This results in data loss. They gain access to every files and documents which are confidential. They put down websites. to avoid the above said problem the proposed system uses AI, where it blocks the hackers and virus introducers into the system by sending back the virus to the introducers.

Related Work

There have been several approaches at either edge of a network. However, a user must communicate with servers inside a service provider to get the content. Thus, the expected performance gain is limited because it can just shortenthe time to generate dynamic content at origin servers inside the service provider.

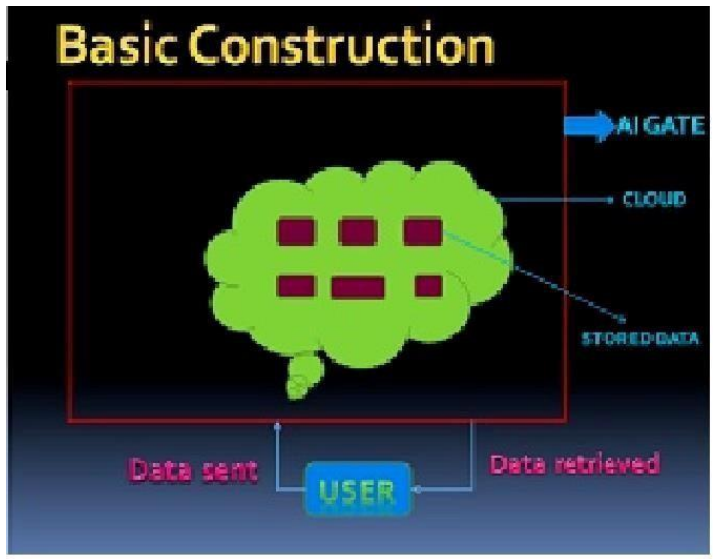

Fig 1: Basic construction of MANETS without AI

In the Fig 1, it is the simple MANETS construction and how the user retrieves and sends the data to and from the MANETS. Herethe data is not secured in order to any of the user can retrieve and send the data to the MANETS.

Why use AI for Cluster?

As security is most demanding in WSN now, we are concentrating on cluster. Cluster data storing is the biggest and emerging trend in the market now. Large data can be stored in cluster. Nowadays everything gets uploaded to server.So we are providing AI security to Cluster. But not only for cluster, can one provide AI security to other fields. AI provides the security in two levels and checks for the bugs and virus for every given period of time.

Why use AI for Cluster?

As security is most demanding in WSN now, we are concentrating on cluster. Cluster data storing is the biggest and emerging trend in the market now. Large data can be stored in cluster. Nowadays everything gets uploaded to server.So we are providing AI security to Cluster. But not only for cluster, can one provide AI security to other fields. AI provides the security in two levels and checks for the bugs and virus for every given period of time.

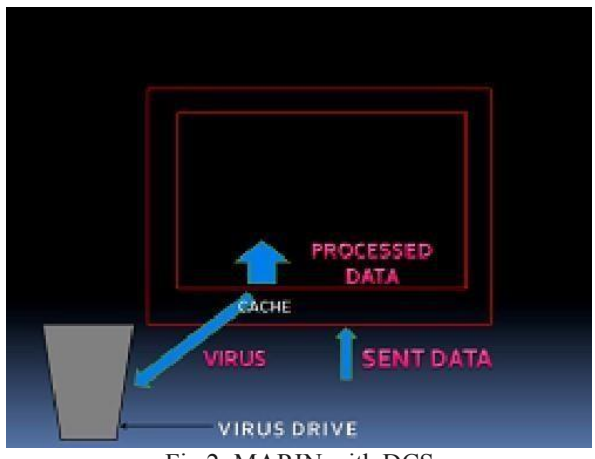

Fig 2: MARIN with DCS

Why use DCS for Cluster?

A method of pre-fetching dynamic content on each client, i.e., a mobile terminal. By using this method, the response time could be shortened if the same user accesses the same content repeatedly. However, other users who want to getthe same content still have to communicate with origin servers to get the data.

How MARIN with DCS works?

MARIN basically consists of a Cluster, AI Coat with a Gate. MARIN provides a coat on Cluster which scans everydata through AI. When the user sends the data through AI gate, it checks for any virus. If any virus is found it removesthe virus and sends it to the virus drive.
Now the data gets stored in the cluster. Every given period of time AI scans for the virus, because there may be somein-built virus in the cluster and it removes then sends to the virus drive.
Cache is placed between the two gates of AI, so that it serves the data the user in a faster rate by means of perfecting method. In order to improve performance, a special cache system with dynamic content pre-fetching in between the two gates of AI. In-network Caching with Dynamic Content Perfecting As shown in Fig. 2, we implemented innetworkcache and pre-fetching system named "Pre-fetching Server" nearby users. To improve the responsiveness and reuse the same dynamic content by multiple users, this system provides the following functions.

1) Caching function: The server stores both static and some types of dynamic content which has been received from origin servers and directly serves users' requests instead of fowarding the requests to the origin servers.
2) Pre-fetching function: The server, on behalf of users, fetches in advance dynamic content which users mightwant to get, later.
Data drive also plays a key role here. When any hacker tries to break in to the AI gate or try transferring any viruses. The AI tracks down the hacker's location, and sends the viruses which are stored from the drive to their system. Now, when the user of MARIN wants to retrieve the data, it asks for a password. The one more key thing about the passwordis that, the password changes for every minute and when the user wants to retrieve the data, the latest password is entered, which is generated by OTP(One Time Password).When the data is retrieved, AI gate again checks for any viruses and checks for any data loss. If everything is fine, the data is retrieved by the user.

Main purpose of MARIN with DCS

- It serves as a main purpose of security of confidential data.
- It can be used in defense to secure their information such as their nuclear missile activation code, their weapon construction, special forces people information.
- MARIN can be used in industries to secure their product information. In software companies to secure theirprograms, and in other field also.
- As it can be used not only for cluster and for other field also, it can be used by everyone.
- It speed up the data transfer by increasing the responsiveness of the dynamic content by using cache segmentation as in case of static content of the sensor nodes It avoids the data breach as it uses the techniqueof AI coat.
- It provides the security against the virus by introducing the virus drive between the cluster nodes and the user.

Services provided by MARIN

Basic user

In this level public will be provided our service where they can keep their data. In this the password can be changedby the user. The user can retrieve data by typing the given password.

Advanced user

In this we provide service to defence people where they can keep their high confidential data without a threat by cyber criminals. In this, the data will get automatically get scrambled once it goes through AI gate which can be only decrypted by typing a key that user has, which is secondary key. The primary key is used to only retrieve data. The retrieved data will be encrypted and it can be decrypted by giving secondary key. The primary passwordchanges every day. Daily scanning is done for more security.

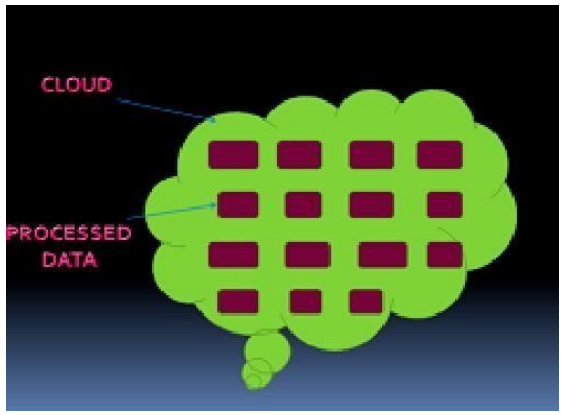

Fig 3: The processed data in MANETS by using AI and DCS

Advantages

1. MARIN with DCS solves 6 security issues out of 9 security issue and some of the challenges of WSN.
2. The system never crashes.
3. Using Artificial Intelligence itself is a big advantage.
4. No need to think about system security as no person can hack AI.

Conclusion

WSN is widely evolving field where security is much more needed. Through our proposed theory we are giving a new dimension for cluster security. Security of the cluster can be improved by trusted computing. MARIN is like Chlorine, which cleans water by removing bacteria, similarly MARIN which cleans MANETS by removing viruses. MARIN with DCS increases the performance of the cluster, faster access of data and increases the life time of the sensor nodes.

References

[1] "An AIS-based MANETS Security Model" Xufei Zheng, Yonghui Fang International Conference on Intelligent Control and Information Processing August 13-15, 2010 - Dalian, China.

[2] "The importance of mandatory data breach notification to identity crime" Eric Holm, Geraldine Mackenzie, Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2014.

[3] P. Padmanabhan, L. Gruenwald, A. Vallur, and M.Atiquzzaman, ―A survey of data replication techniquesfor mobile ad hoc network databases,‖ VLDB J., vol. 17, no. 5, pp. 1143–1164, Aug. 2008.

[4] A. Derhab and N. Badache, ―Data replication protocols for mobile ad hoc networks: A survey andtaxonomy,‖ IEEE Commun. Surveys Tuts., vol.11,no. 2, pp. 33–51, Second Quarter, 2009.

[5] Australia. Australian Government, Discussion Paper: Australian Privacy Breach Notification. Barton: Attorne.