ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

A Security Framework for Distributed Denial of Service Attacks (DDoS) Detection on Wireless Sensor Networks in Smart Cities

M.Sweatha, Dr.S.Vijayalakshmi

Research Scholar, Department of Computer Science, Sri Ramakrishna College of Arts and Science for Women, Coimbatore, India

Associate Professor, Department of Computer Science, Sri Ramakrishna College of Arts andScience for Women, Coimbatore, India

ABSTRACT: A wireless sensor network (WSN) can act as one type of core smart city infrastructure. Smart grids, smart transportation, smart government and so on can all be realized using WSNs. The security of WSNs is a key issue for smart cities so to enhance the security of sensor network a security framework is developed. Wireless sensor network cannot defend against Distributed Denial of Service attack so to detect and protect the attack a security framework is proposed. Mean based Weighted for Quaternion Firefly Algorithm is proposed to detect DDoS attack on Wireless Sensor Network in Smart Cities.

KEYWORDS: MANET, Wireless Sensor Networks, DDoS, MWQFA.

I.INTRODUCTION

Mobile Ad Hoc Network is a self-organizing and self-configuring multi-hop wireless network, the network structure changes dynamically due to member mobility [1]. The nodes are free to move randomly and organize themselves arbitrarily thus the network's wireless topology may change rapidly [2].One of the applications of MANET is Wireless sensor networks [3].

A wireless sensor network is type of wireless network. It is small and infrastructure less basically wireless sensor network consist a number of sensor node called tiny device and these are working together to detect a region to take data about the environment [4].

A Wireless Sensor Network (WSN) can act as one type of core smart city infrastructure [2][6]. Smart grids, smart transportation, smart government and so on can all be realized using WSNs [7]. Therefore the security of WSNs is a key issue for smart cities.

Wireless sensor network cannot defend against Distributed Denial of Service attack so to detect and protect the attack a mechanism is proposed. The DDoS attack can break into wireless sensor networks and disrupt their normal task which leads to network traffic and packet loss.

To enhance the security of WSNs a security framework is proposed in this research work that protect against DDoS attack.

II.LITERATURE REVIEW

P. Yi et al "Green firewall: An energy-efficient intrusion prevention mechanism in wireless sensor network"

Wireless sensor networks (WSNs) are vulnerable to security attacks due to the broadcast nature of transmission and limited computation capability. After an intrusion detection system (IDSs) identifies a mobile intruder, IDS may broadcast the blacklist to all nodes in network. An energy efficient intrusion prevention mechanism is developed in WSNs called green firewall. It can isolate an intruder with less overhead and track the intruder to continually prevent the attack [5].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

K.Ota et al "Dynamic Itinerary Planning for Mobile Agents with a Content-Specific Approach in Wireless Sensor Networks"

Mobile Agents still remains unfledged in development of application-oriented data fusion in wireless sensor networks. A dynamic itinerary planning for MAs (DIPMA) is proposed to collect data from sensor networks with an application-oriented approach. The DIPMA algorithm is applied to the data collection for frost prediction which is a real-world application in agriculture using sensor networks [6].

L. Guo et al "Proposed Security Mechanism for XMPP-Based Communications of ISO/IEC/IEEE 21451 Sensor Networks"

A security mechanism is proposed that deals with the requirements of authentication, integrity, confidentiality, nonrepudiation, access control is proposed. Ensuring security of communications over XMPP is one of the most important issues in ISO/IEC/IEEE21451-1-4 sensor networks. The XMPP-based communications in ISO/IEC/IEEE 21451 sensor networks utilize the username/password security token and role-based access control technologies[7].

W. Kanoun et al "Success Likelihood of Ongoing Attacks for Intrusion Detection and Response Systems"

Intrusion detection and response systems with risk analysis or cost-sensitive approaches combined to enhance the detection and the response procedure.The Risk has two primary dimensions: (i) the likelihood of success of the attacks, and (ii) the impact of the attacks and the countermeasures [8].

III.EXISTING WORK

3.1 PROBLEM SPECIFICATION

In smart citiesongoing attacks with mutable attributes and unknown attacks with novel features are sophisticated persistent threats that disturb the normal functions of WSNs. A framework is proposed using UCON and chance discovery. Software-Defined Networking (SDN) and Network Function Virtualization (NFV) are used to perform attack mitigations [12][13].

3.2 METHODS ADOPTED

3.2.1 Chance Discovery Theory

Chance discovery theory is intended to detect attacks. The purpose of chance discovery is to understand the meaning of rare events to help users make decisions to protect the system from risks [9].

3.2.2 Usage Control (UCON)

UCON performs data control not only at the time of access but also during and after use. Continuous decisions with regard to data access can be made before the access is allowed during a user's session or even after the session ends[10].

3.3 DISADVANTAGE OF EXISTING WORK

- UCON framework is less security and quality of service parameters in WSN is not satisfied.
- Analysis of unknown attacks in WSNs becomes difficult.
- High chance of getting Distributed Denial of Service Attacks (DDOS) attacks easily.

IV.PROPOSED WORK

In this work propose a security framework based on Mean based Weighted for Quaternion's Firefly Algorithm (MWQFA) is proposed to improve the security of WSN .A mechanism is developed to protect against Distributed Denial of Service (DDoS) in Wireless Sensor Network.

4.1 FLOWDIAGRAM OF PROPOSED WORK

In the initial stage of the work network formation is done using MATLAB simulator. At initially the network model is represented as the key graph model using key graph algorithm. Once the nodes in the networks are connected

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

to each other they can access data from the server. While accessing data there may be more chances of threats in the network which cannot be known where the attack is affected.So to detect the attack in the network, each node maintain routing table which stores all information.

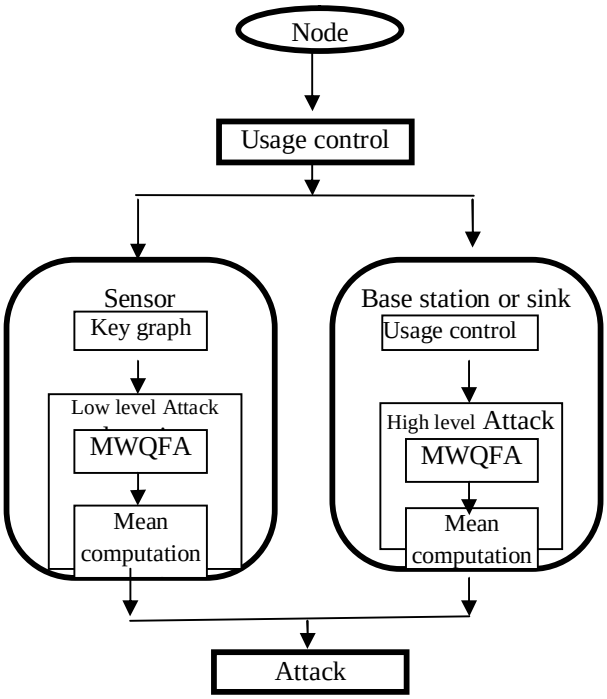

Figure 4.1 Flow diagram of MWQFA-UCON

Once the network formation is done next stage of the work path selection is done in network model to access the data. The packets are transferred from source to destination using shortest path.

4.2 MEAN BASED WEIGHTED FOR QUATERNIONS FIREFLY ALGORITHM (MWQFA)

Mean based Weighted for Quaternions Firefly Algorithm (MWQFA) is used to detect the attacks in the network. Usage Control (UCON) performs data control before and after accessed by users. The attacks in the networks can be detected quickly by MWQFA-UCON. Attack Mitigation techniques are performed to prevent against attacks.

This work presents a new intrusion detection mechanism for DDoS detection. DDoS attacks based on weakness are classified into vulnerability and flood attacks. Firefly Algorithm (FA) as being one of the more famous representatives of this class of algorithm. Fireflies are insects, the main characteristic of which is their flashing lights that can be admired in the summer sky at night. The flashing lights intensity I decrease as the distance r increases according to the term $I \alpha I/r^2$to formulate the FA. To avoid premature convergence in FA algorithm introduce a quaternion's representation. In mathematics, quaternions extend complex numbers.

The fitness value is determined based on the standard deviation value of the features.

The MWQFA is based on the original FA, where the representation of virtual fireflies is moved from a space to a quaternion Mahalanobis- distance space.

In the Mahalanobis- distance, each virtual firefly is represented as D-dimensional real-values nodes vector$N = (n_1, .. n_N)$, where $N_{ij} \in \mathbb{R}^n$, while in quaternion space as a D-dimensional vector of quaternions

$q_i = \{q_{i0}, ... q_{in}\}$, where $q_{ij} \in \mathbb{H}^n$.

The quaternion $q \in \mathbb{H}$ describes a 4-dimensional space over the real numbers.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

V.RESULTS

In this section the simulation results of some metrics are considered and evaluated.In this work 100 numbers of nodes are initialized and created for evaluation. The following metrics are taken in this work they are

- **Path delay**
- **Throughput**
- **Packet Delivery Ratio**
- **Packet Loss Ratio**
- **Execution Time**

5.1 PATH DELAY

It is defined the average time taken by a data packet to arrive in the destination for particular path. It also includes the delay caused by route discovery process and the queue in data packet transmission.

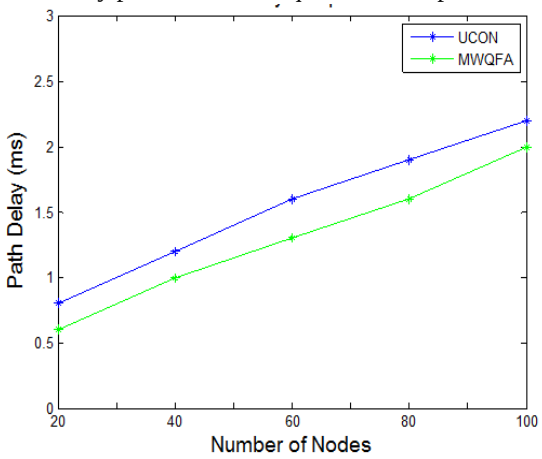

Fig5.1 Path delay result comparison

5.2 THROUGHPUT

Throughput comparison with respect to time is measured based on the following formula.

$$Throughput = \frac{Packet\ received}{amount\ of\ packet\ forwarded}$$

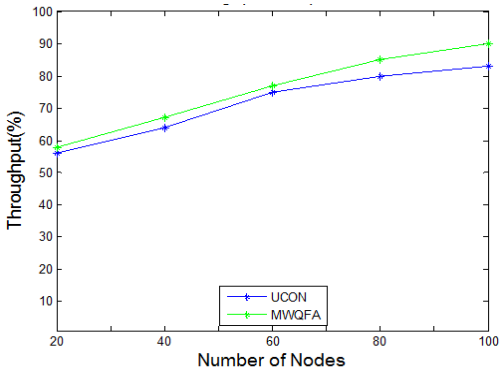

Fig 5.2 Throughput result comparison

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

5.3PACKET DELIVERY RATIO

Packet delivery ratio is defined as

$$PDR = \frac{Number\ of\ packet\ receive}{Number\ of\ packets\ \ arrived}$$

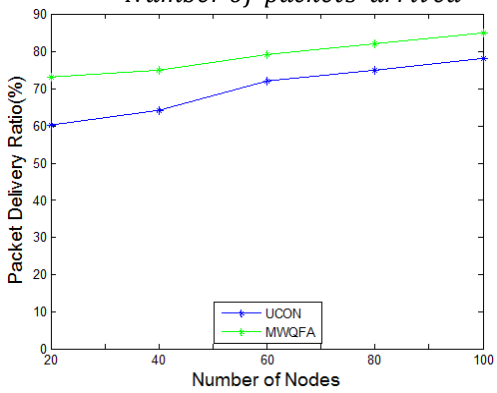

Fig5.3 Packet Delivery Ratio result

5.4 PACKET LOSS RATIO (PLR)

Packet Loss Ratio (PLR) is defined as subtracting the value of PDR to 100 to the destination.

$$PLR = 100 - PDR$$

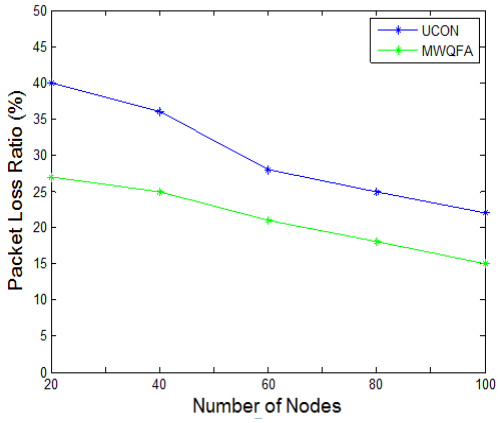

Fig5.4 Packet Loss Ratio result comparison of MWQFA & UCON

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

5.5 TIME

The time execution is the average time span between the time a sensor receives a request and when it makes a local detection decision.

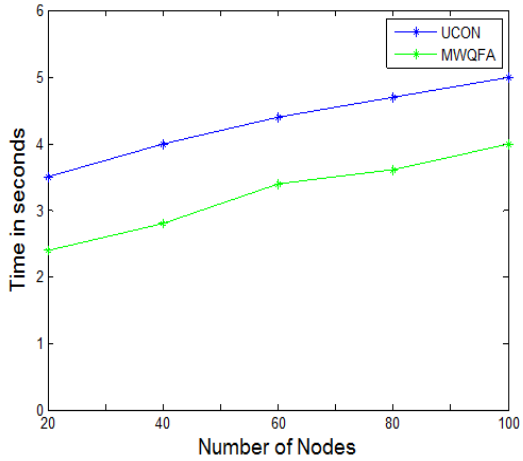

Fig5.5 Time result comparison of MWQFA & UCON

VI.CONCLUSION

The security is a key issue in WSN for smart cities so to enhance the security of sensor network a security framework is developed. The WSN cannot prevent against DDoS attack so to detect against attacks a mechanism is proposed.

In this work a Distributed Denial of Service (DDoS) attack is protected using Mean based Weighted for Quaternions Firefly Algorithm (MWQFA).In the future work can combine features of different technologies.

REFERENCES

1. JeorenHoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester "An Overview of Mobile ad hoc Netwroks: Applications& Challenges".
2.Senthilkumar P., Baskar M. and Saravanan K., "A Study on Mobile Ad-Hock Networks (MANETS)", JMS, Vol. No.1,Issue No.1, September 2011.
3.Aarti and Dr. S.S Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", IJARCSSE International Journal of Advanced Research in Computer Science and Software Engineering, V ol. 3, May2013.
4. Akyildiz, Ian F, and Mehmet Can Vuran.Wireless sensor networks. John Wiley & Sons, 2010
5. Yi, P., Zhu, T., Zhang, Q., Wu, Y. and Li, J., "Green firewall: An energy-efficient intrusion prevention mechanism in wireless sensor network", In Global Communications Conference.
6. Ota, K., Dong, M., Wang, J., Guo, S., Cheng, Z. and Guo, M., "Dynamic itinerary planning for mobile agents with a content-specific approach in wireless sensor networks", IEEE 72nd Vehicular Technology Conference Fall.
7. Guo, L., Wu, J., Xia, Z. and Li, J., "Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks", IEEE Sensors Journal, 15(5), pp.2577-2586,2015.
8. Kanoun, W., Cuppens-Boulahia, N., Cuppens, F., Dubus, S. and Martin, A., "Success likelihood of ongoing attacks for intrusion detection and response systems", International Conference on Computational Science and Engineering (CSE'09), Vol. 3, pp. 83-91, 2009.
9. Y. Ohsawa and P. McBurney, Eds., Chance Discovery (Advanced Information Processing). New York, NY, USA: Springer-Verlag, 2003.
10. X. Zhang, F. Parisi-Presicce, R. Sandhu, and J. Park, "Formal model and policy specification of usage control", ACM Transaction Information System Security., vol. 8, no. 4, pp. 351-387, 2005.
11. Z. Su, Q. Xu, H. Zhu, and Y. Wang, "A novel design for content delivery over software defined mobile social networks", IEEE Networking., vol. 29, no. 4, pp. 62-67, 2015.
12. R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: A survey",IEEE Communication Magazine, vol. 51, no. 11, pp. 24-31.