Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.874 – 878

RESEARCH ARTICLE

MULTI TARGET TRACKING USING IDOL IN SENSOR NETWORKS

M.Navanidha, PG Scholar, Dept of IT, SNS College of Technology, Coimbatore

V.Nirosha, Assistant Professor, Dept of IT, SNS College of Technology, Coimbatore

mnavanidha@gmail.com

ABSTRACT: The target tracking is one of the most important applications of wireless sensor networks. When nodes operate in a duty cycling mode, tracking performance can be improved if the target motion can be predicted and nodes along the trajectory can be proactively awakened. This will negatively influence the energy efficiency and constrain the benefits of duty cycling. A Probability-based Prediction and Sleep Scheduling protocol (PPSS) to improve energy efficiency of proactive wake-up. Based on the prediction results, PPSS then precisely selects the nodes to awaken and reduces their active time. A target prediction scheme based on both kinematics rules and theory of probability, PPSS not only predicts a target's next location, but also describes the probabilities with which it moves along all the directions. The single target tracking is carried out. Multi Targets are to be tracked in next phase. Using Centralized Device, the Network is to be monitor and the security is to be provided.when nodes operate in single target tracking,the tracking performance can be low transmission delay, high energy consumption and less network lifetime. In the proposed system, multi target tracking are used. The IDOL techniques is used to identify, detect and localize the target.Two sensor nodes are used easy to sensing and to detect the target.By using these technique to improve the energy efficiency and network lifetime. The result revealed that the proposed methods effectively to increase the energy efficiency compared to the existing methods. IDOL system is to localize attackers. Simulation is performed in Network Simulator.Spoofing prevention mechanism will be incorporated in future.

Keywords: Sensor Networks, Localization, Energy Efficiency, Network Lifetime

1. INTRODUCTION

1.1 WIRELESS NETWORK

A wireless network uses wireless network connection. It eliminates the costly process of laying cables into any building like homes, telecommunication network. Wireless network uses Radio waves to connect devices such as laptops to the internet. Wireless medium is open.A wireless network is a system for connecting a computer to a network without the use of cabling. In its simplest form it consists of a computer with a wireless card and a wireless router. Wireless Network enables computers to be connected without the use of cabling to a server, hub or switch. Various types of attacks can affect wireless networks.

Wireless systems are prone to many type of attacks because of the openness of the wireless network. A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data or bypass access controls. There are several different types of spoofing attacks that malicious parties Some of the most common methods include IP address spoofing attacks and DNS server spoofing attacks. A spoofing attack can affect hosts, switches, and routers connected to your Layer 2 network by sending false information to the devices connected to the subnet.

Energy is the scarcest resource of WSN nodes, and it determines the lifetime of WSNs. WSNs are meant to be deployed in large numbers in various environments, including remote and hostile regions, where ad hoc communications are a key component. For this reason, algorithms and protocols need to address the following issues:

- Lifetime maximization
- Robustness and fault tolerance
- Self-configuration

Lifetime maximization: Energy/Power Consumption of the sensing device should be minimized and sensor nodes should be energy efficient since their limited energy resource determines their lifetime. To conserve power the node should shut off the radio power supply when not in use.

If a centralized architecture is used in a sensor network and the central node fails, then the entire network will collapse, however the reliability of the sensor network can be increased by using a distributed control architecture. Distributed control is used in WSNs for the following reasons:

- Sensor nodes are prone to failure,
- For better collection of data
- To provide nodes with backup in case of failure of the central node
- There is also no centralised body to allocate the resources and they have to be self organised.

1.2 Benefits of Wireless Networks

- Convenience
- Mobility
- Productivity
- Easy setup
- Expandable
- Security Cost

Wireless Networks are prone to many types of attacks and exploitation. Spoofing attacks are common types of attacks. Spoofing Attacks can be launched with little effort as the wireless medium is shared. Spoofing attack occurs when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware

2. TECHHNIQUE USED

Many conventional techniques were used to prevent spoofing attack. Conventional methods were used also to determine which node is being affected. Main disadvantage of conventional method is overhead requirement & it doesn’t have ability to localize the positions of the adversaries after attack detection. Spatial information is a physical property associate with each node. This spatial information is used for,

- Determining the multiple attack.
- Determining number of attackers when many attackers masquerading as the same node identity.
- Localizing multiple opponents.

IDOL is used to localize multiple adversaries .In this technique easy to determine the detect and localize the target. One key observation is that IDOL can be handle attackers using different transmission power levels, thereby providing strong evidence of the effectiveness of localizing adversaries when there are multiple attackers in the network. It provides the strong evidence of high accuracy of localizing multiple adversaries.

3. RELATED WORK

IDOL, an integrated detection and localization system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels. chosen a set of representative localization algorithms ranging from nearest neighbor matching in signal space**.**

Received Signal Strength (RSS) is used to detect MAC spoofing. MAC address can be easily spoofed in wireless LANs. RSS may vary from attacker node & original node. Algorithm based on AM was used to detect attack. RSS measurement is mainly dependent on distance between transmitter & receiver, so it can mainly be used for location determination[2].

In Alignment Prediction Alignment is used to predict the RSS values during trace reconstruction. In Trace Reconstruction two RSS classes are obtained in each time interval. One belongs to the victim node & other belongs to the spoofing node. In this the main objective is to reconstruct two RSS traces in time window**.**

The problem of determining the number of attackers is formulated as a multi-class detection problem. Two cluster-based mechanisms to determine the number of attackers was first proposed. An integrated detection and localization system that can localize the positions of multiple attackers was developed**.** RSS is widely available in deployed networks and its values are closely correlated with location in physical space. In addition, RSS is a common physical property used by a widely diverse set of localization algorithm

4. EXISTING SYSTEM

The Existing System consists of,

Energy efficiency is a critical feature and the purpose of extending the network lifetime.

Idle listening is a major source of energy waste.

Proactive wakeup simply awaken all the neighbour nodes.

Single target tracking only.

Time delay and energy consumption occur.

The idea of duty cycling is to put nodes in the sleep state for most of the time, and only wake them up periodically. In certain cases, the sleep pattern of nodes may also be explicitly scheduled, i.e., forced to sleep or awakened on demand. This is usually called sleep scheduling.

The drawback here is there may be a chance of having single target tracking and awakened all nodes due to network failure of traffic and wastage of energy.

To reduce communication costs some algorithms remove or reduce nodes redundant sensor information and avoid forwarding data that is of no use. As nodes can inspect the data they forward they can measure averages or directionality for example of readings from other nodes. For example, in sensing and monitoring applications, it is generally the case that neighbouring sensor nodes monitoring an environmental

5. PROPOSED SYSTEM

The proposed system consists of,

To improve the efficiency of proactive wakeup.

Reducing the number of awakened nodes and controlling their active time.

To run on individual nodes, improve the scalability.

Reduce the time delay and energy consumption.

Multi target tracking is used to track particular time to given nodes.

When the number of attackers will cause failure in localizing the multiple adversaries. To use the same identity node to launch attacks, determining the number of attackers becomes a multi class detection problem and its similar to determining in the RSS readings. It based on averaged RSS from each node identity inputs to estimate the position of nodes. when RSS readings of both the original node as well as spoofing nodes of different physical locations.

The scene matching localization algorithm uses the interpolated signal map, which is built from a set of averaged RSS readings with known(x,y)locations. In area based depend only on their some supported areas. It is a multi lateration algorithm that encodes the signal to distance propagation model.

Localization of target nodes is a fundamental problem in wireless sensor networks. Up to now, the most existing localization algorithms of WSNs can be classified into two categories are range-based and range-free. Range-based algorithms use distance or angle estimates in their location estimations. Range-free algorithms use connectivity information between unknown nodes and anchor nodes. Range-based localization algorithms need to measure the actual distances or orientation between adjacent nodes, and then use the measured data to locate unknown nodes.

6. PERFORMANCEEVALUATION

When adversaries using different transmission power levels. To evaluate the performance of our approach by using the difference of returned medoids. Adversaries used the same transmission power level, changed the power level and compared original node.

1.Impact of Thresold and sampling number: the thresholds of test statistics define the critical region for the significance testing. However the averaged variance decreases with the increasing number the samples.

2.Handing different transmission levels: If a spoofing attacker sends packet a transmission power level from the original node based on the cluster analysis in RSS cluster analysis.

3.Performance of detection: To use integrated system to detect attacks as well localize the position of adversaries. Then use the leave out method in localize algorithm, to choose one location as a testing node whereas the rest of the location as training data till all the location have been tested.

7. CONCLUSION AND FUTURE WORK

PPSS improves the energy efficiency with an acceptable loss on the tracking performance. it is difficult to configure the protocol toward the best energy performance trade-off for a specific network environment. The prediction method of PPSS cannot cover special cases such as the target movement with abrupt direction changes. Received signal strength based spatial correlation is used**.**In addition to cluster analysis to achieve better accuracy of determining the number of attackers based on the number of attackers determined by our mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing strong evidence of the effectiveness of the approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries.

Future Work:

Without performance constraints, it is difficult to configure the protocol toward the best energy-performance trade-off for a specific network environment. The Centralized device is used to monitor the network. By using multi target easy to reduce the time delay and energy efficiency. Whenever the abrupt direction changes takes place in multi target easy to determine the attackers and to identify, detect and localise the multiple target.

REFERENCES

[1]Jie yang,ying ying chan,wade trappe,jerry cheng "Detection and localization of multiple spoofing attackers in wireless networks"IEEE transaction on parallel and distributed system vol24 jan-2013

[2]Ding chau wang,chao chun chen and chen han liao "Communication Efficient tracking model selection methods multi model based object tracking sensor networks"International journal of innovative computing,information vol 9 mar 2013

[3]Chandrasekaran.G,Francisco.J,Ganapathy.V,Gruteser.M,Trappe.W,2009),'DetectingIdentity Spoofs in IEEE 802.11eWirelessNetwork'IEEEGLOBECOM.

[4]Chen.Y, Trappe.W, and Martin.R.P, (2007), "Attack Detection in Wireless Localization," Proc. IEEE INFOCOM, Apr. 2007.(SECON)

[5]Chen.Y,Trappe.W,andMartin.R.P,'DetectingandLocalizingWirelessSpoofingAttacks,'Proc.Ann.IEEE Comm. Soc.Conf. Sensor**,**(2006) Mesh and Network..

[6]Faria.D and Cheriton.D,(2006),Detecting Identity-Based Attacks in NetworksUsingSignalprints' Proc.ACM Workshop Wireless Security

[7]Ferreri.F,Bernasch.M,andValcamonic.L,(2004),'AccessPointsVulnerabilitiesto Dos Attacks in 802.11 Networks,'Proc.IEEE Wireless Comm. and Networking Conf.

[8]Li.QandTrapp.W,(2006),'Relationship-Based Detection of Spoofing-Related Anomalous Traffic in Ad Hoc Networks,'Proc. Ann. IEEE Comm. Soc. on IEEE Conf.

[9]Li.Q and Trappe.W, (2007),' Detecting Spoofing and Anomalous Traffic in Wireless Network via Forge Resistant Relationships 'IEEE transactions on information and security, Vol. 2.

[10]Madigan.D,Elnahrawy.E , R. Martin, Ju.W, Krishnan.P, and Krishnakumar.(2005), 'Bayesian Indoor Positioning Systems', Proc. IEEE INFOCOM, pp.324-331.

[11]Sheng.Y,Tanand,K,Campbell.A,(2008) 'Detecting 802.11MAC Layer
Spoofing Using Received Signal Strength',Proc. IEEE Infocom.

[12] Wang.K ,(2007), 'Estimating the Number of Clusters via System Evolution for Cluster Analysis of Gene Expression Data', Technical Report NO. 2007-258,Computer Science Dept., Xidian Univ., P.R. China.