Dynamic Reputation Value For CCN In Mobile Networks

V.Keerthiga[1], S.Bargunan[2], G.Bharathikannan[3]
[1, 2] Dept of CSE
[2, 3]Assistant Professor, Dept of CSE
[1, 2, 3] Sembodai Rukmani Varatharajan Engineering College

Abstract- *As a new generation of network architecture with subversive changes to traditional IP networks, Content Centric Networks (CCN) has attracted widespread attention from domestic and foreign scholars for its efficient content distribution, multi-path and secure routing features. The design atchitecture of CCN network has many advantages. However, it is also easily used illegally, which brings certain sectrity problems. For example, objectified network resources which include requesters, publishers, content, and node routes , are faced with many security threats, such as privacy attribute disclosure, privacy detection, content information disclosure, and spoofing and denial of service attacks. A node routing security scheme based on dynamic reputation value is proposed for the security problem of node routing. It is convenient for detecting node routing attacks and defending in time. And it could provide security for the Content Centric Networks node routing without affecting the node routing advantages and normal user requests.*

Keywords- content centric networks; security issues; dynamic reputation value; defensing; routing advantages

I. INTRODUCTION

Wireless sensors, and the arrangement of these small, electronic devices into radio networks, have introduced the capability of remotely monitoring a physical environment for a wide variety of parameters. In effect, there is additionally the ability to interface the physical world, monitoring whatever parameter is of interest, with the internet.

Mobile Wireless Sensor Network

Mobile wireless sensor networks (MWSNs) can simply be defined as a wireless sensor network (WSN) in which the sensor nodes are mobile. MWSNs are a smaller, emerging field of research in contrast to their well-established predecessor. MWSNs are much more versatile than static sensor networks as they can be deployed in any scenario and cope with rapid topology changes .With the development of MEMS and robotic techniques, mobile sensors are realized by putting in sensing devices on mobile platforms.

Hybrid Wireless Device Network

Hybrid wireless device networks (WSNs) that consist of such mobile sensors and conventional static sensors, open new frontiers of WSN analysis. Mobile sensors have more powerful sensing and computing capabilities. They can move to specific locations to hold out missions such as replacement broken nodes or analyzing suspicious events. Adding quality to a WSN considerably improves its ability and reduces the deployment and maintenance costs. We are interested in the situation of dispatching “multi-attribute” mobile sensors to the locations of events showing within the sensing field. Static sensors are responsible for reporting wherever suspicious events appear. Mobile sensors then move to those event locations to conduct in-depth analysis. Given a group of attributes A, each event reported by static sensor(s) is associated with one attribute in A. Mobile sensors are equipped with multiple sensing devices, therefore every of them will analyze multiple attributes of events.

Multi-Attribute Mobile Sensor

Multi attribute mobile (MAM) sensors. However, MAM sensors may have different attributes. When an event of attribute $a_i \in$ A is reported by static sensor(s), only the MAM sensors with attribute a_i can be dispatched to analyze that event.

II. RELATED WORK

Task Allocation In MRSs

MRS is one research topic in robots, which adopts multiple cooperative robots to accomplish a specific task in the uncertain environment .develop multi-agent reinforcement learning schemes to train robots to learn the mappings between their statuses and actions. Obviously, these studies have different objectives from our paper. Multi-robot task allocation, on the other hand, considers assigning multiple tasks to a team of mobile robots. Each task indicates a target location required to be visited by one robot, and the objective is to minimize the total cost (for example, the moving distance of all robots).

Sensor Maneuver In WSNs

Several research efforts investigate how to move mobile sensors to adjust the network topology for some purposes. moves sensors to approximate the distribution of events and maintain complete coverage of the sensing field. After identifying coverage holes, to move sensors to fill these holes. Both adopt virtual forces among sensors to make them evenly distribute over the sensing field. After computing the locations to place sensors investigate how to dispatch sensors to these locations in an energy-efficient manner. This issue is similar to the sensor dispatch problem, but they consider minimizing the energy consumption of sensors in only one round. Mobile sensors have also been considered to track moving objects. Given targets in a mobile WSN addresses how to move sensors to improve the quality of tracking a target, while avoid potential breakage of network connectivity and reduce the loss of sensing coverage due to sensor movement.

III. PROPOSED METHODOLOGY

The CCN network implements the process of communication from "host-host" to "request content acquisition content". The main body of the service is content, not storage location. Unlike traditional IP networks, node routing can cache content information in order to shorten the information request time and improve communication efficiency. CCN's special architectural design and unique advantages have attracted the attention of attackers while being widely concerned by the academic community. The hidden danger zone in the architecture is used to attack and steal private information on various objects in the network. At present, academic research on CCN network content mostly focuses on caching and routing. There is not much research on its security and privacy. The object of the requester, information dissemination, content, and other network node routing resources are still faced with many issues of privacy and security

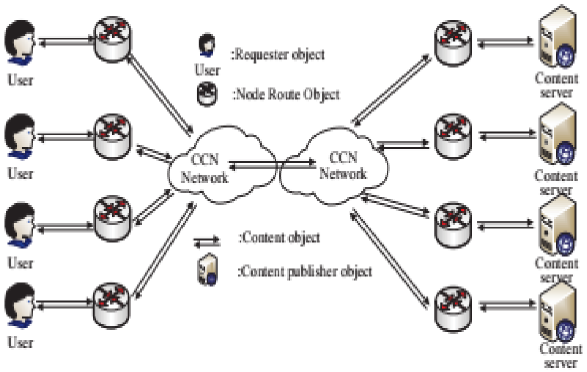

Fig 3.1: System Architecture

Advantages

- To provide security for the node routing without affecting the request of the legitimate user.
- Network traffic scales with the content creation rate rather than the content consumption rate as in the current network
- Hosting data is as simple as naming the data and providing a CCN node which indicates it can fulfill requests for the data name
- To shorten the information request time and improve communication efficiency.

Another advantage of this configuration is that small mobile robots are inexpensive and thus can be employed in larger numbers. To enable cooperation within the team, the robots have communication abilities and the parent robot is able to teleoperate the child robots within its line-of-sight. Similar team configurations were presented. For many robotic tasks, a model of the environment is a necessary prerequisite. Since cameras have become flexible, low-priced and lightweight devices, image-based mapping is an **attractive alternative to** mapping with range sensor especially for robots with limited resources.

IV. SYSTEM IMPLEMENTATION

SYSTEM MODULE

The System Modules are

- CCN Network Formation
- Node Routing
- Protection Mode
- Defense Function Algorithm

MODULES DESCRIPTION

CCN Network Formation

During the communication process, the request packet is issued by the content requester and arrives at the node route. The packet is returned if the interest request content is already cached in the node route. Otherwise, node-routed broadcast or default port forwarding is used. The request packet continues to be passed until the interest packet arrives at the content server, and the content server returns the content data packet. According to the different roles of various resources in the CCN network, CCN network resources can be divided into different objects such as content requester, content publisher, content, and node routing.

Node Routing

The request and release of content information in the CCN network is the basis of the communication of the service subject[9~10]. Communication between subjects is guaranteed only if the consistency of the process between the requester object and the publisher object is guaranteed. And these depend on the node routing object is relatively safe. Currently, the security problems of node routing include resource exhaustion, timing attacks, interference attacks, and flooding.

Protection Mode

The request and release of content information in the CCN network is the basis of the communication of the service subject[9~10]. Communication between subjects is guaranteed only if the consistency of the process between the requester object and the publisher object is guaranteed. And these depend on the node routing object is relatively safe. Currently, the security problems of node routing include resource exhaustion, timing attacks, interference attacks, and flooding.

Defense Function Algorithm

The defense mechanism algorithm of the node routing object consists of two parts: (1) delay mechanism, (2) cooperative defense. The delay mechanism mainly uses each node routing object to have an ILU collection, and the collection contains the abnormal node user marked as the attack object. Node routing generates a random delay for each node user through a delay generation algorithm. The node responds immediately to a user interest request that is not considered an attacker. The routing response to two different requester nodes is shown in the figure below. When the legitimate user U1 requests the node to cache the content, it will get a timely response. When a U 2 request is made by an illegal user, it is delayed for a certain period of time. In the collaborative defense, the node route sends a cooperative defense data packet to the neighboring node to inform the attacker of the information. The neighboring node automatically parses the data packet after receiving such a cooperative data packet, and obtains the marked illegal user. Check the ILU table in the node. If such a node already exists, forward the cooperative packet through the broadcast or default port. Otherwise the node user information is added to the ILU U table

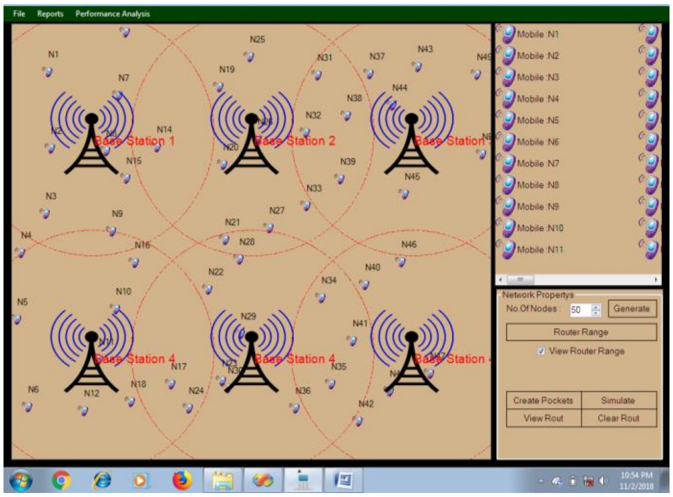

Fig A 2.1: View The Number of Node Available.

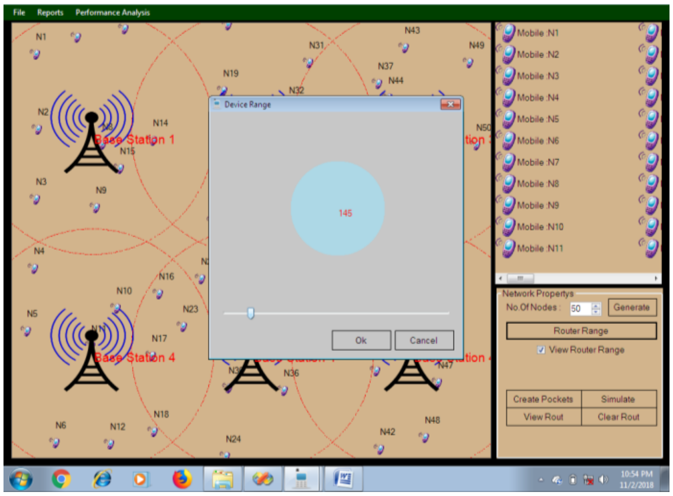

Fig A 2.2: Node Details.

V. CONCLUSION AND FUTURE WORK

The CCN network resources are divided into different objects according to their roles in the network. Faced with different network resource objects for security analysis, it highlights several types of attacks faced by node routing objects in the network. For the attack of the node routing object, a node routing security scheme is proposed, which aims to provide security for the node routing without affecting the request of the legitimate user. The routing response to two different requester nodes is shown in the figure below. When the legitimate user U1 requests the node to cache the content, it will get a timely response. When a U 2 request is made by an illegal user, it is delayed for a certain period of time. In the collaborative defense, the node route sends a cooperative defense data packet to the neighboring node to inform the attacker of the information. The neighboring node automatically parses the data packet after receiving such a cooperative data packet, and obtains the marked illegal user. Check the ILU table in the node. If such a node already exists, forward the cooperative packet through the broadcast or default port. Otherwise the node user information is added to the ILU U table.

VI. ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to my college management. I would like to give my thanks to guide who gave me the golden opportunity to do this wonderful project on the. In addition, I would also like to thank my parents who helped me a lot in finalizing this project within the limited time frame.

REFERENCES

[1] You-ChiunWang, "A Two-Phase Dispatch Heuristic to Schedule the Movement of Multi-Attribute Mobile Sensors in a Hybrid Wireless Sensor Network," Mobile Computing, IEEE Transactions on , Vol: 13, no: 4, pp: 709- 722, 2014.

[2] Tseng .Y.C , Wang Y.C and Wu. F.J , "Mobility management algorithms and applications for mobile sensor networks," Wireless Comm. and Mobile Computing, vol. 12, no. 1, pp. 7–21, 2012.

[3] Song .A, Song .G , Wei .Z , and Zhang .W, "A hybrid sensor network system for home monitoring applications," IEEE Trans. Consumer Electronics, vol. 53, no. 4, pp. 1434–1439, 2007.

[4] Cheng .K.Y, Hsieh Y.Y , Tseng .Y.C, and Wang .Y.C , "iMouse: an integrated mobile surveillance and wireless sensor system," Computer, vol. 40, no. 6, pp. 60–66, 2007.

[5] Cheng L, Wu .C.D, and Zhang Y.Z, "Indoor robot localization based on wireless sensor networks," IEEE Trans. Consumer Electronics, vol. 57, no. 3, pp. 1099–1104, 2011.

[6] Bartolini . N ,Calamoneri . T, La Porta . T.F, and Silvestri. S, "Autonomous deployment of heterogeneous mobile sensors," IEEE Trans. Mobile Computing, vol. 10, no. 6, pp. 753–766, 2011.

[7] Benjamin .M.R ,Eickstedt .D.P, Leonard . J.J and Schmidt .H, "Adaptive control of heterogeneous marine sensor platforms in an autonomous sensor network," Proc. IEEE/RSJ Int'l Conf. Intelligent Robots and Systems, pp. 5514–5521, 2006.

[8] Ferrari .S, Fierro .R, and Tolic .D, "A geometric optimization approach to tracking maneuvering targets using a heterogeneous mobile sensor network," Proc. IEEE Conf. Decision and Control, pp. 1080– 1087, 2009.

[9] Hofmeister . M, Kronfeld . M, and Zell . A, "Cooperative visual mapping in a heterogeneous team of mobile robots," Proc. IEEE Int'l Conf. Robotics and Automation, pp. 1491–1496, 2011.

[10] Kesidis .G. and Rao . R , "Purposeful mobility for relaying and surveillance in mobile ad hoc sensor networks," IEEE Trans. Mobile Computing, vol. 3, no. 3, pp. 225–231, 2004.

[11] Chang .M.H, Peng .W.C, and Tseng. Y.C and Wang .Y.C, "Exploring loadbalance to dispatch mobile sensors in wireless sensor networks,"Proc. IEEE Int'l Conf. Computer Comm.2007.