International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

A SEMANTIC AND ADAPTIVE APPROACH FOR MOBILE SOCIAL NETWORK USING OPTIMIZATION SCHEDULING ALGORITHM

Satheesh kumar.k[1], Sri Devi.S [2], Savithri.P[3], Renuka.B[4]

[1]Assistant professor, cse department, university college of engineering, Thirukkuvalai.
[2,3]cse department, university college of engineering, Thirukkuvalai.

Abstract - *A Self configuring Network consisting auxiliary customer design in the covered system. Using sensors to monitor physical or environmental conditions. It is more complex to secure the data. Malicious data injections take place when the sensed measurements are maliciously altered to trigger wrong and potentially dangerous responses. Security is one of the most important issues that have attracted a lot of research and development effort in past few years. This technique provides privacy preserving; collusion proof reduced the communication storage overheads.*

***Key Words*: mobile social network, bigdata, security resources, mathching theory, coalitional game.**

1. INTRODUCTION

Recently, with the development of the communication technologies and devices, an ever-increasing amount of mobile social big data are being delivered among mobile social users by various applications, such as multimedia streaming, healthcare services, etc. Especially, with the emerging mobile social networks (MSNs), people in different locations can form communities to exchange and share mobile data**.** For the applications of mobile social big data, security issues should be taken into consideration. For example, the location information is critical to mobile social users as the disclose of location may reveal where, when or even what mobile social users have done. In addition, the wireless connection, which is used by mobile social users to obtain social services, should be protected in order to prevent from being attacked by the third parties. Therefore, except the conventional wireless resource, the security resource such as computation resource to implement monitoring, encryption, etc, is also needed.

However, as the security resource is limited, how to allocate the security resource to deliver mobile social big data becomes a new challenge as follows. On one hand, are with Shanghai Key Laboratory of Power Station Automation Technology, School of Mechanics and Different amount of security resource should be allocated based on different situations such as the level of threats. On the other hand, mobile social users have different social activities with the result that mobile social users also have different security resource demands to obtain social services.

Although some related studies have been carried out to study security issues in mobile networks, most of them mainly focus on how to protect the privacy of mobile social users, instead of the security resource allocation. Next, despite some works related to wireless resource, most of them are to allocate wireless resource such as bandwidth or spectrum without the consideration of security. In addition, the social features of mobile users who deliver the mobile social big data are also needed to be discussed. Therefore, the security-aware resource to deliver mobile social big data is still an open and new issue to be studied.

The matching theory is employed to model the selecting process between communities and the coalitions of BSs, where mobile social users can optimally share the obtained resource with each other. A joint matching-coalition algorithm is proposed to obtain the stable resource allocation.

RELATED WORKS

In [1] N. Kayastha, D. Niyato, P. Wang, E. Hossain et al presents The mobile social network (MSN) combine technique in communal awareness and wireless infrastructure for mobile networking. The MSN can be consider as a system which provide a variety of data delivery services relating the social relationship along with mobile users. These papers current a complete survey on the MSN purposely from the standpoint of applications, system architectures, and protocol propose issues. First, major applications of the MSN are review. Next, different architectures of the MSN are presented. Each of these different architectures supports different data delivery scenario. The one and only distinctiveness of community correlation in MSN give increase to unrelated protocol design issues. This research issue (e.g., community detection, mobility, content distribution, content sharing protocols, and privacy) and the connected approach to address data delivery in the MSN are described. At the end, several significant research directions are outline.

In [2] Q. Xu, Z. Su, and S. Guo et al presents Rapid developments in mobile services and wireless technologies have promoted users to form mobile social networks (MSNs), where bundles can be delivered via opportunistic peer to peer links in a store-carry forward mode. This mode needs all nodes to work in a cooperative way. However, mobile nodes may be selfish and would not be willing to forward data to others due to the limited resources (e.g., buffer, energy etc.), resulting in a degraded system performance. To tackle the above problem, this paper proposes a novel incentive scheme to stimulate selfish nodes

to participate in bundle delivery in MSNs. At first, a virtual currency is introduced to pay for the relay service. Then, a bundle carrier selects a relay node from its friends or other strangers based on its status. Next, a bargain game is employed to model the transaction pricing for relay service. In addition, the simulation results show that the proposal can improve the performance of the existing schemes significantly. Mobile social networks (MSNs) have emerged, where mobile users can create and share their content with each other, by using mobile devices equipped with short range wireless interfaces via peer to peer opportunistic links

In [3] L. Xiao, C. Xie, T. Chen, H. Dai, H. V. Poor et al presents Mobile devices, such as smart phones, can offload applications and data to the cloud via access points or base stations to reduce energy consumption and improve user experience. However, mobile offloading is exposed to smart attackers that use smart and programmable radio devices, such as universal software radio peripherals, to perform multiple types of attacks, such as spoons and jamming, based on the radio location and offloading transmissions. In this paper, a mobile offloading game is investigated that consists of three players: a mobile device that chooses its offloading rate, a smart attacker that determines its attack mode, and a security agent that decides whether or not to initiate full protection for the serving access point during the offloading. In dynamic radio environments. Simulation results show that the proposed offloading strategy can improve the utility of the mobile device and reduce the attack rate of smart attackers. The large number of cloud-based mobile services, mobile devices such as Smartphone and tablets can offload their applications and data to the cloud to improve user experience in terms of longer battery lifetime, larger data storage, faster processing speed and more powerful security services.

In [4] Z. Su, Q. Xu, M. Fei and M. Dong et al presents The rapid increases in both the population of mobile social users and the demand for quality of experience (QoE), providing mobile social users with satisfied multimedia services has become an important issue. Media cloud has been shown to be an efficient solution to resolve the above issue, by allowing mobile social users connecting it through a group of distributed brokers. However, as the resource in media cloud is limited, how to allocate resource among media cloud, brokers and mobile social users becomes a new challenge. Therefore, in this paper, we propose a game theoretic resource allocation scheme for media cloud to allocate resource to mobile social users though brokers. Firstly, a framework of resource allocation among media cloud, brokers and mobile social users is presented. Media cloud can dynamically determine the price of resource and allocate its resource to brokers. Mobile social user can select his broker to connect media cloud by adjusting the strategy to achieve the maximum revenue, based on the social features in the community.

In [5] L. Xiao, D. Xu, C. Xie, N. B. Mandayam et al presents Cloud storage is susceptible to superior Persistent Threats (APTs), in which an assailant launches stealthy, continuous, well funded and targeted attacks over storage devices. In this paper, we affect viewpoint theory (PT) to prepare the communication flanked by the protector of a cloud storage system and an APT attacker who makes subjective decisions that sometimes deviate from the results of the expected utility theory, which is a the basis of traditional game theory. In the PT-based cloud storage defense pastime with pure-strategy, the protector decide a examine gap for each storage device and the slanted APT attacker chooses his or her attack interval against each device. A mixed approach prejudiced storeroom resistance game is also investigated, in which each of the subjective defender and APT attacker acts under uncertainty about the action of its opponent.

PROPOSED SYSTEM

In the proposed system to detect anomalies in the network. The trust management techniques are to keep track of a sensor's cooperation in time, assigning it a trust value. In the proposed system a novel methodology implemented in the sensor network. The Main concept of this project is identifying the misbehaving node in the network.

MODULES

- Set Up Phase
- Packet Transmission Phase
- Audit Phase
- Detection Phase

SET UP PHASE

This phase takes put right after route PSD is established, but prior to any data packets are transmitted over the route. In this phase, S decide on a symmetric-key crypto-system encrypt key; decrypt key and K symmetric keys key1; . . . ; key K, where encrypt key and decrypt key are the keyed encryption and decryption functions, respectively. S firmly distributes decrypt key and a symmetric key key j to node nj on PSD, for j ¼ 1; . . .;K. Key allocation may be based on the public-key crypto-system such as RSA: S encrypts keyj using the community key of node nj and sends the cipher text to nj. nj decrypts the cipher text by its private key to obtain keyj. S also announces two hash functions, H1 plus HMAC key , to all nodes in PSD. H1 is un keyed while HMAC key is a keyed hash purpose that will be used for message verification purposes later on. Besides symmetric key sharing, S also needs to set up its HLA keys.

PACKET TRANSMISSION

After finishing the setup phase, S enters the packet transmission phase. S transmit packets to PSD according to the following steps. Before distribution out a packet Pi, where i is a sequence number that exclusively identifies Pi, S

computes and generate the HLA signature of ri for node nj, as follows the node has received, and it relays to the next hop on the direct. The last hop, i.e., node nK, only forwards Pi to the destination D. As prove in Theorem 4 in Section 4.3, the special structure of the one-way chained encryption building in (4) dictates that an upstream node on the route cannot get a copy of the HLA cross intended for a downstream node, and thus the construction is elastic to the collusion model defined in Section 3.2. Note that here we think the verification of the integrity of Pi as an orthogonal problem to that of verify the tag tji. If the verification of Pi fails, node n1 should also stop forward the packet and should mark it accordingly in its proof-of-reception file.

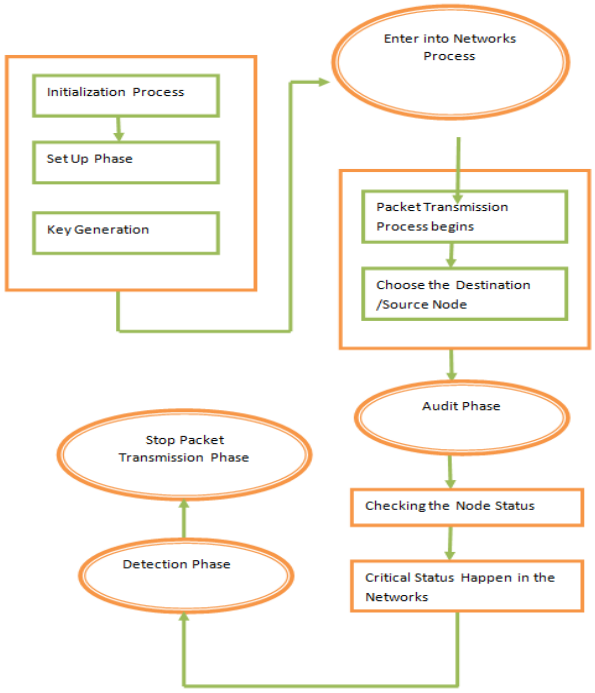
AUDIT PHASE

This phase is trigger when the public auditor Ad receives an ADR communication from S. The ADR message includes the id of the nodes on PSD, ordered in the downstream course, i.e., n1; . . . ; nK, S's HLA public key information, the sequence information of the most recent M packets sent by S, and the sequence statistics of the subset of these M packets that were received by D. Recall that we assume the in sequence sent by S and D is truthful, because detecting attacks is in their attention. Ad conducts the auditing process as follows. Ad submits a random confront where the elements cji's are randomly chosen from Zp. Without loss of generality, let the series number of the packets recorded in the current proof-of-reception file be P1; . . . ; PM, with PM being the most recent packet sent by S. the above device only guarantees that a node cannot understate its packet loss, i.e., it cannot claim the reaction of a packet that it actually did not receive. This mechanism cannot avoid a node from overly stating its packet loss by claiming that it did not receive a packet that it really received.

DETECTION PHASE

The public assessor Ad enters the detection phase after receiving and auditing the reply to its confront from all nodes on PSD. The major tasks of Ad in this phase include the following: detecting any exaggeration of packet loss at each node, constructing a packet-loss bitmap for each hop, scheming the autocorrelation function for the packet loss on each hop, and decide whether malicious behavior is present. Known the packet-reception bitmap at each node, b1; . . . ; ~b K, Ad first checks the constancy of the bitmaps for any possible overstatement of packet losses. Clearly, if to hand is no overstatement of packet loss, then the set of packets received at node j þ 1 have to be a subset of the packets received at node j. Because a normal node forever truthfully reports its packet reception, the packet-reception bitmap of a malevolent node that overstates its packet loss must contradict with the bitmap of a common downstream node.

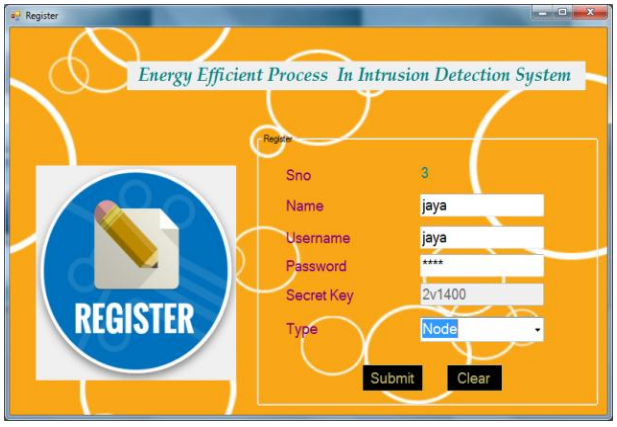
ARCHITECTURE



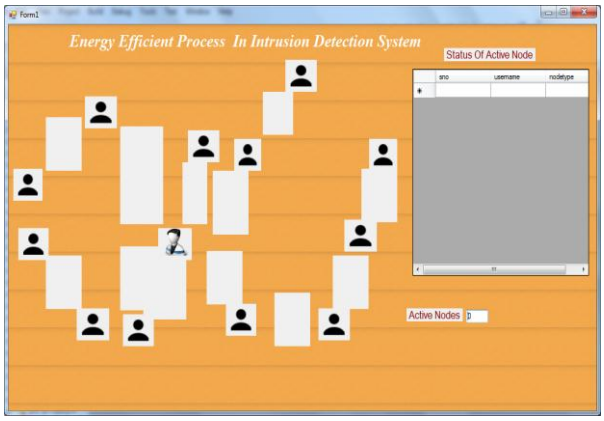
OUTPUT RESULTS

The evaluation of the proposed scheme is done by comparing the performances of the IDSs under two scenarios: (a) keeping IDSs running throughout the simulation time and (b) using our proposed scheme to reduce the IDS's active time at each node in the network. From the simulation results, to observe that the effectiveness of the IDSs in the network is not compromised while using the proposed scheme, rather, there is considerable reduction of energy consumption in each of the nodes that increases the network lifetime significantly. Here we have assumed a homogeneous network in a way that all the nodes have the same capacities in terms of their computational and energy resources.

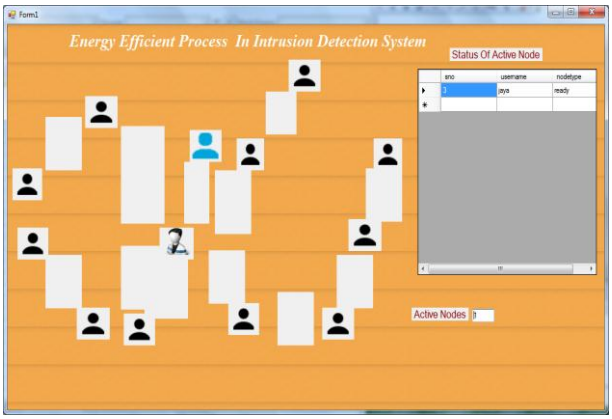
Node Entry Process



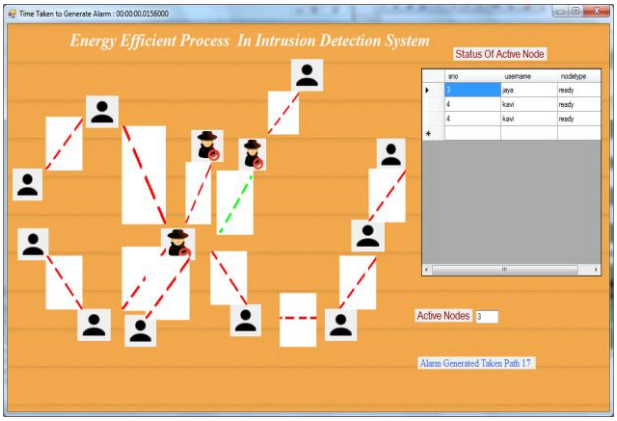
Network Login



Network Process



Hacking Process



CONCLUSION

In the proposed a scheme of security-aware resource allocation based on joint coalition-matching game. In the scheme, both the wireless resource and security resource of the BSs can be allocated simultaneously. Specifically, based on a coalition game model, the BSs can form group to share security resource and determine the price of resource to obtain the profits by providing these resource to mobile social users. Mobile social users can select the optimal coalition to require resource, where the matching theory is used to model the selection process between communities and coalitions. At last, the joint coalition-matching algorithm is introduced to obtain the stable result of security-aware resource allocation. Simulation results have been presented to demonstrate the performance of the proposal. As for the future work, we will investigate the cloud security resource allocation in MSNs to offload the overhead of BSs.

REFERENCE

[1] N. Kayastha, D. Niyato, P. Wang, E. Hossain, "Applications, architectures, and protocol design issues for mobile social networks: a survey," in Proc. IEEE, vol. 99, no. 12, pp. 2130-2158, Dec. 2011.

[2] Q. Xu, Z. Su, and S. Guo, "A game theoretical incentive scheme for relay selection services in mobilesocial networks," IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6692-6702, 2016.

[3] L. Xiao, C. Xie, T. Chen, H. Dai, H. V. Poor, "A Mobile Offloading Game Against Smart Attacks," IEEE Access, vol. 2016, no. 4, pp. 2281 - 2291,2016.

[4] Z. Su, Q. Xu, M. Fei and M. Dong, "Game theoretic resource allocation in media cloud with mobile social networks," IEEE Transactions on Multimedia, vol.18, no.8, pp. 1650-1660, 2016. [5] L. Xiao, D. Xu, C. Xie, N. B. Mandayam, and H. V. Poor, "Cloud Storage Defense Against Advanced Persistent Threats: A Prospect Theoretic Study," IEEE Journal on Selected Areas in Communications, 2017.DOI: 10.1109/JSAC.2017.2659418

[6] Y. Hui, Z. Su, and S.Guo, "Utility Based Data Computing Scheme to Provide Sensing Service in Internet of Things", IEEE Transactions on Emerging Topics in Computing, Jun. 2017, DOI: 10.1109/TETC.2017.2674023

[7] Q. Xu, Z. Su, K. Zhang, P Ren, and X. Shen, "Epidemic Information dissemination in mobile social networks in opportunistic links," IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 3, pp. 399-409, 2015.

[8] J. Ren, Y. Zhamg, K. Zhang, and X. Shen, " Adaptive and Channel- Aware Detection of Selective Forwarding Attacks inWireless Sensor Networks," IEEE Transactions on Wireless Communications, vol. 15, no. 5, pp. 3718-3731, 2016.

[9] Z. Su and Q. Xu, "Content distribution over content centric mobile social network in 5G," IEEE Communication Magazine, vol. 53, no. 6, pp. 66-72, 2015.

[10] Y. Zhang, J. Ren, J. Liu, C. Xv, H. Guo, and Y. Liu, "A survey on Emerging Computing Paradigms for Big Data," Chinese Journal of Electronics, vol. 2016, no. 1, pp.1-12, 2017.