Parallel Load Balancing and Overlay Authentication System for Secure Industrial Network Communications

Lejun Ji, Gang Lei*, Ruiwen Ji, Mengshuang Bao, Hao Liu, and Zhuojun Dong
School of Software, Jiangxi Normal University, Nanchang 330022, China

Abstract

On one hand, being a highly self-establishing wireless network with dynamic topology, mobile ad-hoc networks (MANET) are not constrained by limitations of fixed framework, and as a consequence, MANETs are now used increasingly in a wide range of fields. On the other hand, flexibility, the typical nature of MANET, making all nodes in an uncontrolled environment. Every node despite its situation is equal to have an opportunity to deal with route events causing an unstable performance of the whole MANET system. To deal such an uncertain problem within any MANET system, this paper presents a novel model called Parallel Load Balancing and Overlay authentication System for Secure Ad-hoc Communications. The model is designed to build up an over-layer to MANET system with those nodes in good condition, which is called strong peers in this paper and do the route job to avoid some bad situation like route fail or authentication fail. Simulation results comparing MANET system with and without the help of over-layer are provided to demonstrate the proposed model suitability for secure ad-hoc communications.

Keywords: mobile ad-hoc networks, security, load balancing, overlay authentication

1 Introduction

With the rapidly soaring frequency of myriad information correspondence in this busy society, and also the widespread availability of mobile communicative devices with high-capacity network currently, there is no doubt that mobile ad-hoc networking (MANET) technology enabling wireless devices to dynamically establish networks with high data transmission efficiency as well as considerable convenience [1] [2] [3]plays an increasingly indispensable role as a promising alternative for the form of network connection and mobile communication in today's world.

MANET system [4] [5] nowadays can be found lots of usage by various fields from small-scale commercial conferences to military battlefield communications [6] for those instantaneous and temporary tasks because such systems are always in badly need of some critical techniques including prompt deployment and active configuration excluding a fixed infrastructure installation or a pre-existing central control device. MANETs got those marvelous advantages like dynamic and flexible topology, self-organizing nature, self-healing network capacity and so on, which meets the critical requirements for those peculiar proposes. [7]

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 6, Article No. 6 (November 1, 2020)

*Corresponding author: Department of Management Science and Engineering, School of software, Jiangxi Normal University, 99 Ziyang Avenue, Nanchang City, Jiangxi Province, 330022, China, Tel:+86(0791)88120471, Email: leigang@jxnu.edu.cn

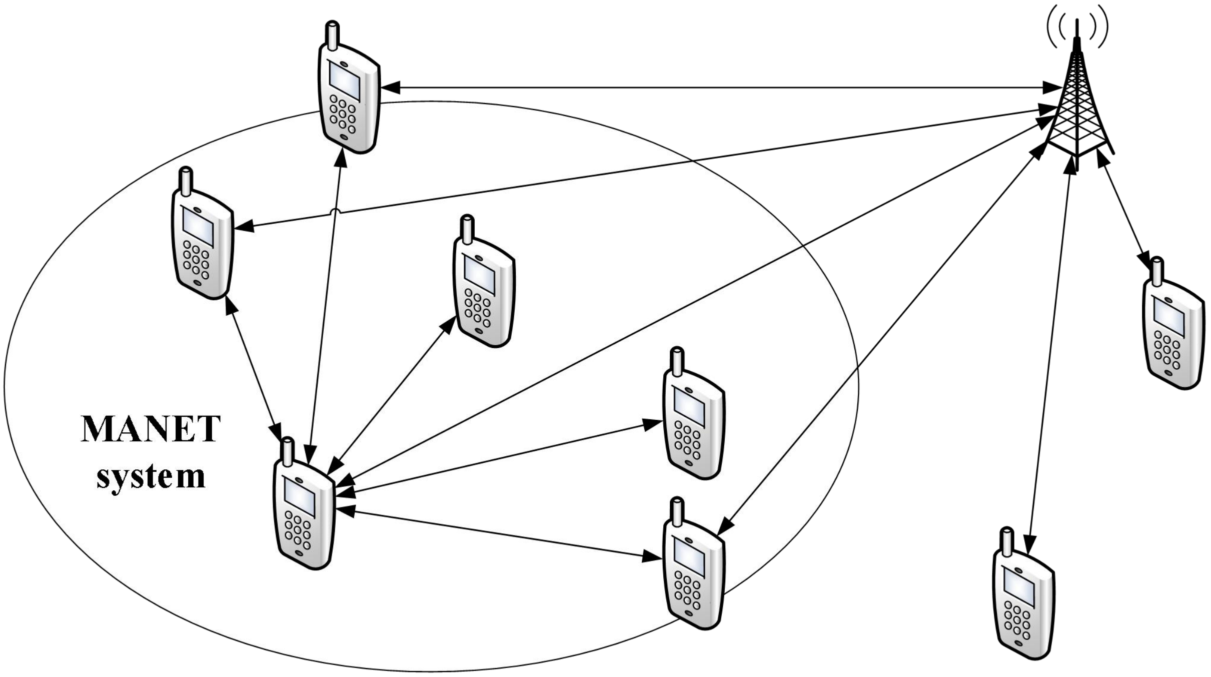


Figure 1: A MANET system overview

As shown in Figure 1, each mobile device within a MANET system is deemed as a node acting equally as not only a client but also a router. Its communication through network is accomplished by dispatching packets from the source node to the destination node, and when a direct source-destination link is unavailable, nodes in between are used as routers, which is also called multi-hop communication [8] [9]. It does mean to be more robust than classic central networks for its information relayed mechanism avoiding cases like a drop of just one node leads to the breaking down of the whole system.

However, as a result of MANET system's flexibility, all the nodes are served as routers, some of which with unhealthy situations (e.g. low battery, low performance, weak signal, function deficiency, etc.) may make a great contribution to a more unstable system [10] [11]. Furthermore, as the fact that wireless communication is the most common way of MANETs' communication, in which could be straightforward eavesdropped on by any node within the system, it's quite indispensable to choose appropriate nodes as routers in defense of the problem device.

This paper proposes a novel ad-hoc model for secure ad-hoc communications (SAC), the parallel load balancing and overlay authentication (PLBOA) system for SAC. The system is designed to be in contrast to the existing route data loading and ad-hoc systems authenticating approaches, which merely provide a single-node layer exposing to such a great number of potential threats that requiring more human intervention to resolve the security problems [12].

The remainder of this paper is organized as follows: Section 2 explains our system detail design for secure ad-hoc communications. Section 3 draws conclusions from the research findings as well as discusses the further work.

2 System Detail Design

2.1 Strong peer-based over-layer construction scheme

As is the fact that the traditional way to manage MANET system is just having all nodes taking part into the system controlling regardless of any probable problems containing lowering computing power, decelerating processes, stressing energy cost, etc. Figure 2 illustrates the MANET system in the traditional way. It’s those problematic nodes pushing the whole system into a dilemma, running still but wastefully, that the main problem we need to settle down. [13] [14] [15]

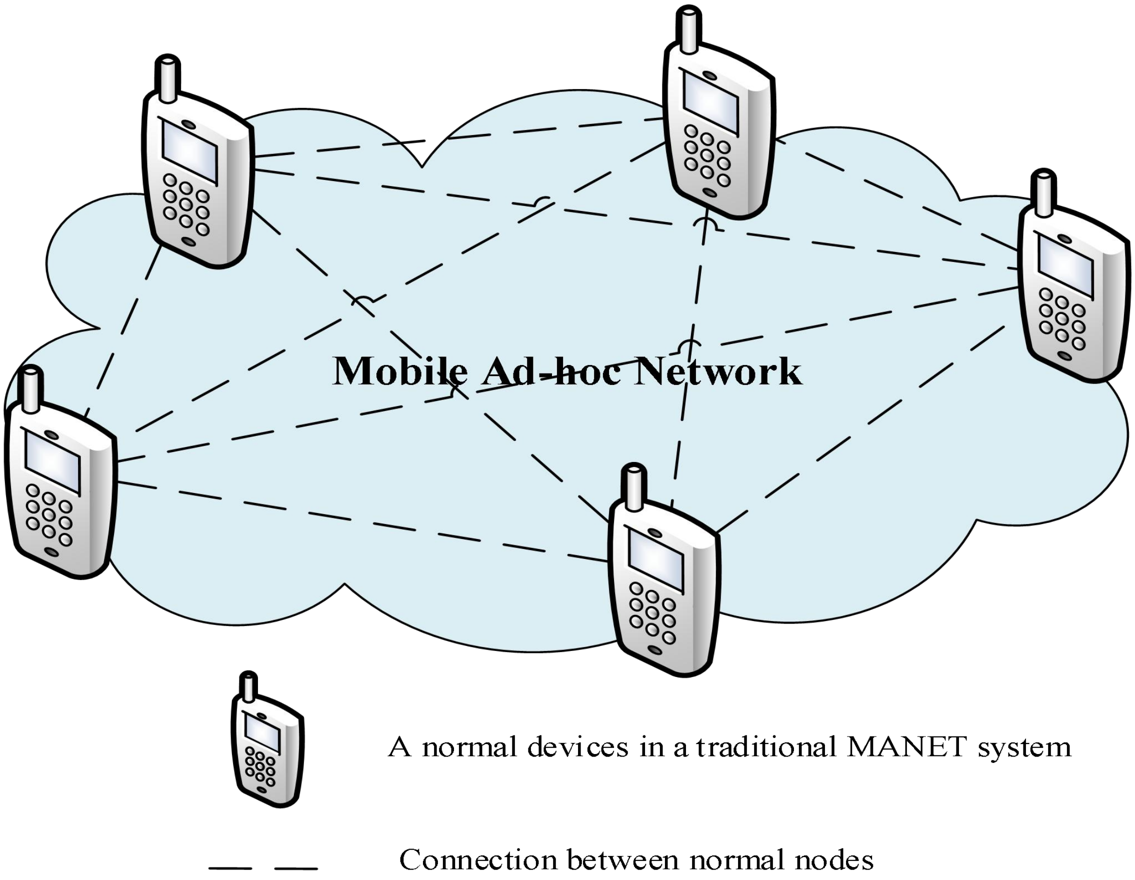

Mobile Ad-hoc Network
A normal devices in a traditional MANET system
Connection between normal nodes

Figure 2: A traditional MANET system

To solve the problems mentioned above, we propose the strong peer-based over-layer construction scheme. The PLABO system with an over-layer full of strong peers can be illustrated like Figure 3. The scheme holding the main idea that cautiously choose the strong peers, the healthy nodes within the system, to build up the over-layer. With such an over-layer, only those strong peers have to take the responsibility to serve as routers and also in this circumstance, the over-layer seemed to be a verifying entrance doing the authentication job.

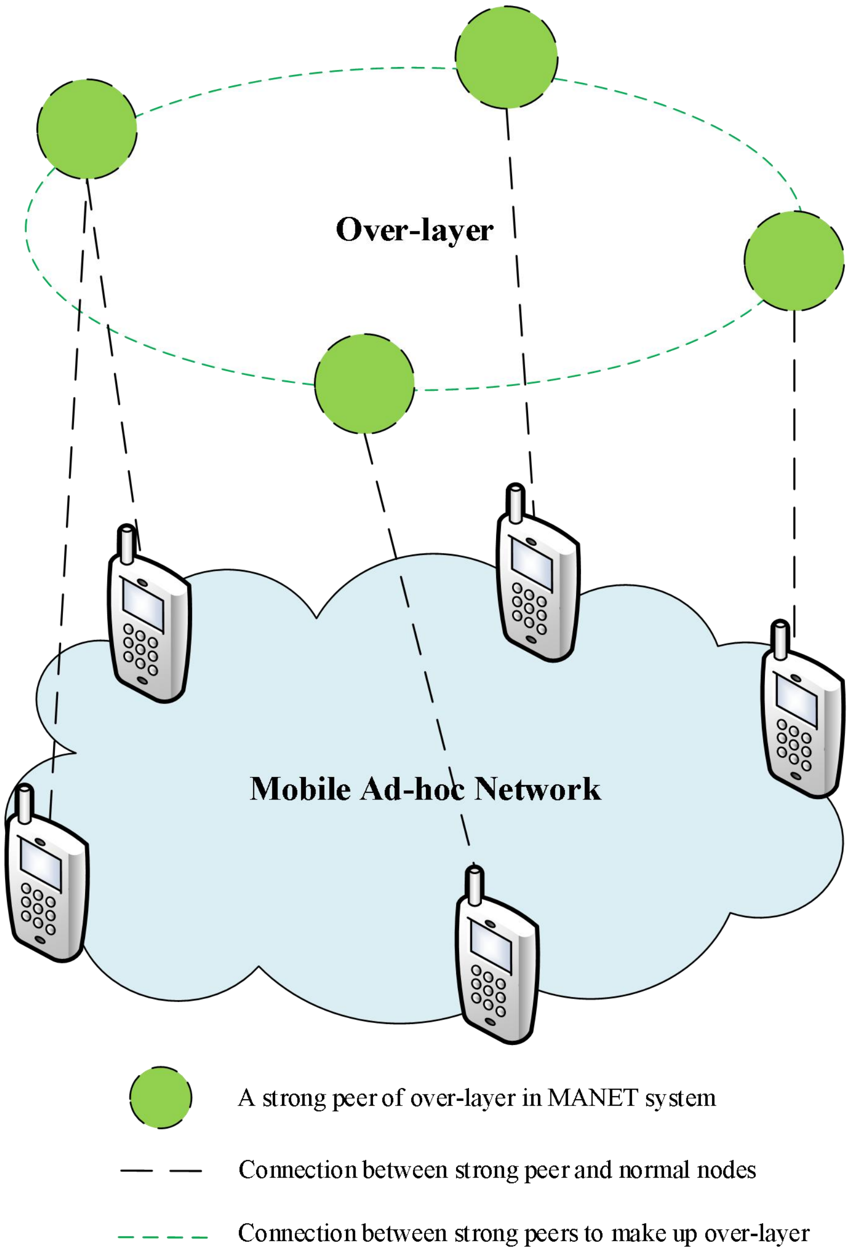

Over-layer
Mobile Ad-hoc Network
A strong peer of over-layer in MANET system
Connection between strong peer and normal nodes
Connection between strong peers to make up over-layer

Figure 3: An overview of the MANET system with an over-layer

Algorithm 1 Strong peer-based over-layer construction scheme

```
Definition:
$P_{list}$:all nodes from the MAENT system
$SP_{list}$: a set of strong peers from the MANET system
$I_r$:the standard strong peer recommended index
$F$(x):strong peers indentification algorithm
for ($i = 1, i \leq$ count($P_{list}$), $i++$) do
    if ($F(P_x) \geq I_r$) then
        add $P_x$ to $SP_{list}$;
    end if
end for
for ($k = 1, k \leq$ count($SP_{list}$), $k++$) do
    take the $S_x$ into over-layer of the MANET system;
end for
    deploy the over-layer in the MANET system;
```

In order to choose those strong peers to make up of the over-layer, it's necessary to take situations of the nodes within the system into consideration. For example, we can suppose $B(x)$ as the remaining battery percent, $R(x)$ as RAM capacity, $N(x)$ as network signal strength, and also $C(x)$ as CPU utilization rate and $P(t)$ as its performance, then we have come up with an algorithm likes

$$F(x)=\alpha\ B(x)+\beta\ \frac{R_r(x)}{R_t(x)}\ +\gamma N(x)+\ C(x)P(x) \qquad (1)$$

where $F(x)$ represents the recommended index of the device x to become a strong peer. The remaining RAM capacity is represented by $R_r(x)$ and respectively the total one by $R_t(x)$, with both of which we can work out the usage rate of RAM. In addition, the unit we use to consume $N(x)$ is dBm, which is always a negative number while the less it is the better signal it means. As for , and are all experiment parameters.

2.2 Hash-based assignment distribution algorithm

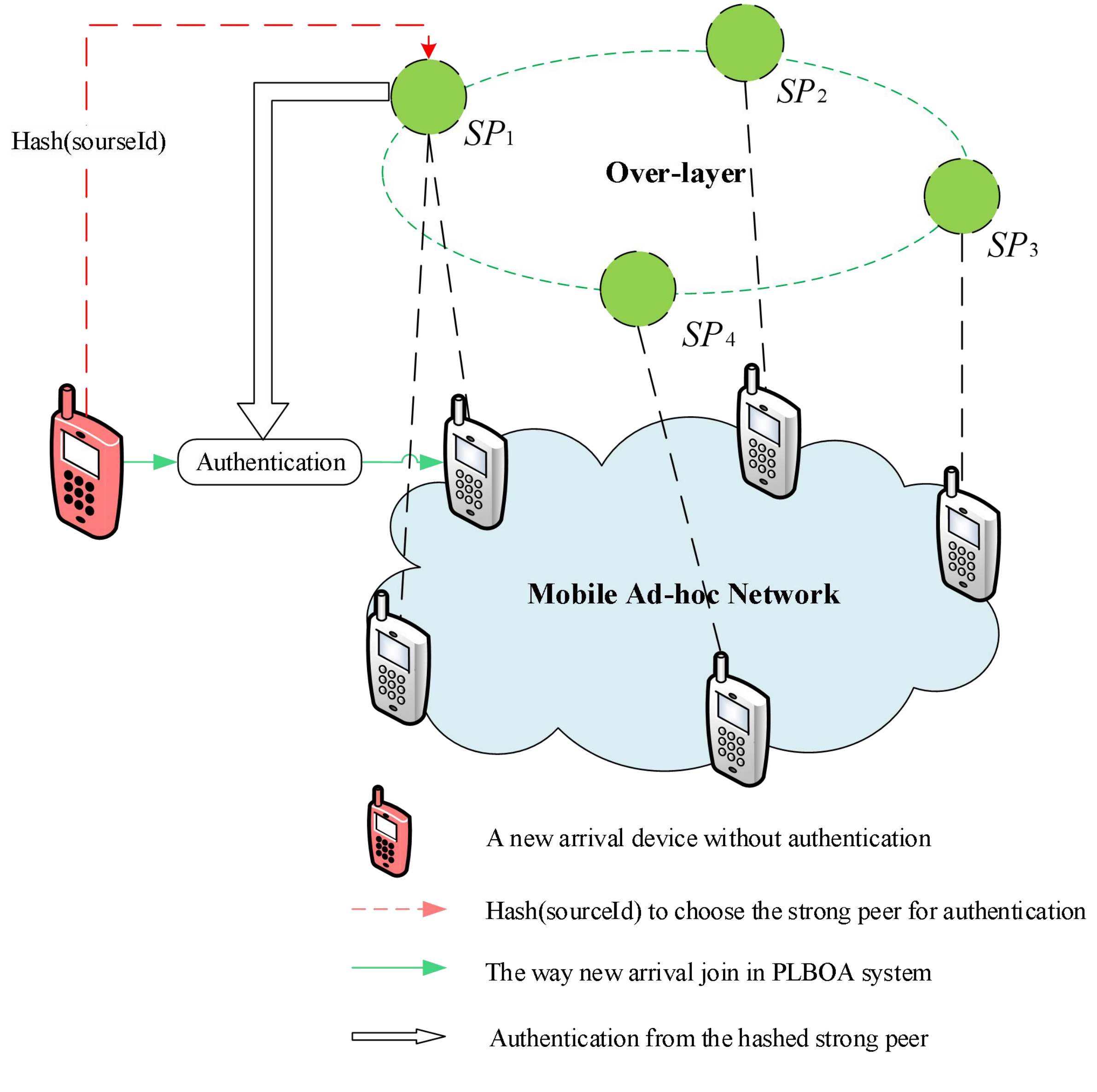
With the strong peer-based over-layer construction scheme (SPOCS) acting as our very fundamental standard to choose those strong peers making up the over-layer, we right now are able to have those dependable devices for the whole system to do many things. Just take what we are going to talk about as an example, it's quite important for us to work out in what order distributing the new arrival nodes to those strong peers of over-layer for authentication. And the method to choose strong peer for those jobs is called hash-based assignment distribution algorithm (BADA) here.

Without BADA we cannot make sure of an identical opportunity for each strong peer being used for new arrival nodes' authentication. Only work it out can we ensure those strong peers' high utilization and full performance of their capacity under control, and as a result, to deal with this it's undoubtedly the prime choice to using a hash function. In this case, just by means of hashing the source IP address from those new arrival devices, we can easily manage to make the new arrival devices authenticated in a parallel load balancing way.

Figure 4 illustrates how we manage to authenticating new arrival nodes by hashing its source IP address. Given that the number of strong peers in this PLBOA system is N, now we can mark them as $SP_1 ... SP_N$.Furthermore, we suppose the source IP of the device to hash as *SrcIP*. Here is the hash function we proposed

$$hash(SrcIP) = SrcIP \bmod N \qquad (2)$$

where we use an common hash function by a modulo operation to get the value of *hash(SrcIP)*,which is also the mark of strong peer (SP_x) chosen to deal with the new arrival node authentication issue.



Hash(sourseId)
SP1
SP2
SP3
SP4
Over-layer
Authentication
Mobile Ad-hoc Network
A new arrival device without authentication
Hash(sourceId) to choose the strong peer for authentication
The way new arrival join in PLBOA system
Authentication from the hashed strong peer

Figure 4: an over-layer with hash-based assignment distribution

As for data packets distribution, we can surely use the strong peers to deal with issues like distributing the data packets, which is also one of the BADA. Every time a strong peer receive data packets from outside, it will analyze the packet to find out information like source IP part as well as destination IP part. Only if these IP match the one of the destination device of the MANET can the packet continue to be transmitted to the corresponding device.

Algorithm 2 Hash-based assignment distribution algorithm

```
Definition:
    $SP_{list}$ : a set of strong peers from the MANET system
    $NP$ : the new arrival device to the MANET system
    $P$acket$_x$ : the packet sent to MANET system
Once having a $NP$ come to MANETs
    use (2) to get the strong peer $SP_x$ to authentication
    if($SP_x$ authenticated)then
        $NP$ join in MANETs
    end if
Once having a $P$acket$_x$ come to MANETs
    use (3) to get the strong peer $SP_x$ to deal with packets
    if(hash mapped rightly)then
        transmit $Packet_x$ to the corresponding device
    end if
```

With the router strong peer to process packets to guarantee the security of the MANET, now in order to ensure the high efficiency of the whole system, it's essential for us to make the whole process running in a parallel way. Just the same as the above algorithm, we can easily make it come true by hashing the source IP of the data packet.

As what is illustrated in Figure 5, we are obviously told that how we realize data packets distribution with our strong peers. We firstly mark those strong peers in the MANETs as $SP_1...SP_N$.Respectively, we do the same thing to the source IP of those data packets (Packet$_1$...Packet$_n$) sent to the MANETs as $SrcIP_1...SrcIP_n$.Then we have our hash function to deal with the data packets

$$hash(SrcIP_x) = SrcIP_x \, mod \, N \qquad (3)$$

where we get the value of $hash(SrcIP_x)$,the mark of the strong peer data packet Packet$_x$ will send to. In this way every data packet will be mapped to a specific strong peer. Then they can set out to the analysis and transmission job.

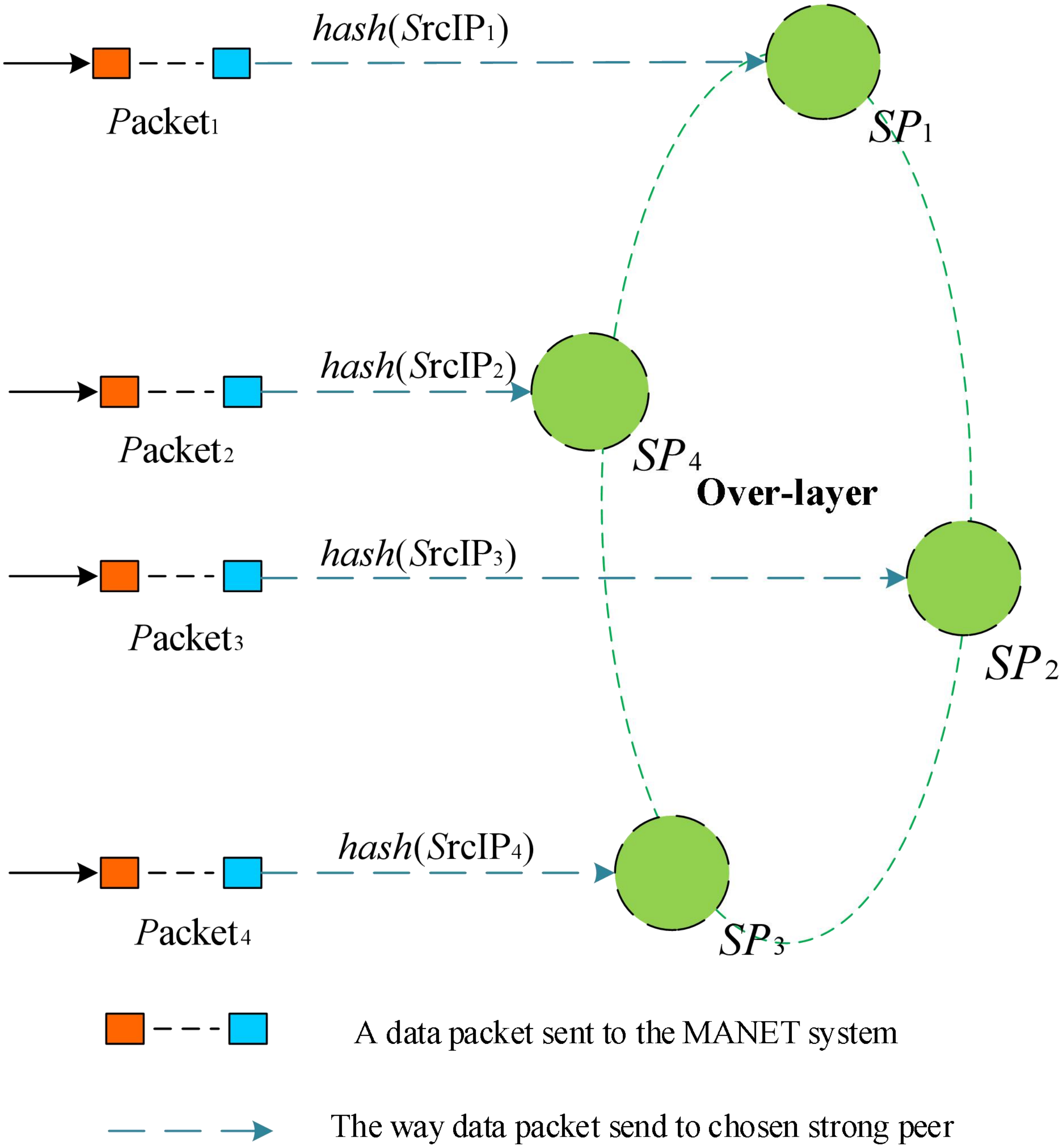


Figure 5: an over-layer with hash-based assignment distribution

3 Conclusions

We present a novel model called Parallel Load Balancing and Overlay authentication System for Secure Ad-hoc Communications. The model is designed to build up an over-layer to MANET system with nodes in good condition, which is called strong peers in this paper and do the route job to avoid some bad situation like route fail or authentication fail. Simulation results validate our design ideas and provide useful guidance for the next detailed evaluation of other transmission performances.In addition, with the rapid development of the wireless communication technology [16] [17], the multipath transmission mode is more and more popular because of multi-path concurrent transmission's characteristics. On the basis of this model, we will follow the current research trends and combine mobile adhoc network (MANET) with Multipath TCP(MPTCP) [18] [19] [20], so it will improve effectively the data transmission efficiency and provide users with an over-layer MANET system,which is more convenient and secure.

References

[1] T. Abdullah, A. Anjum, N. Bessis, S. Sotiriadis, and K. Bertels. Nature inspired self organization for adhoc grids. In *Proc. of the 27th International Conference on Advanced Information Networking and Applications (AINA'13), Barcelona, Spain*, pages 682–689. IEEE, March 2013.

[2] A. Bader and M.-S. Alouini. Mobile ad hoc networks in bandwidth-demanding mission-critical applications: practical implementation insights. *IEEE Access*, 5:891–910, 2017.

[3] S. Batabyal and P. Bhaumik. Mobility models, traces and impact of mobility on opportunistic routing algorithms: A survey. *IEEE Communications Surveys & Tutorials*, 17(3):1679–1707, 2015.

[4] Y. Cao, J. Chen, Q. Liu, G. Lei, H. Wang, and I. You. Can multipath tcp be robust to cyber attacks with incomplete information? *IEEE Access*, 8:165872–165883, 2020.

[5] Y. Cao, S. Chen, Q. Liu, Y. Zuo, H. Wang, and M. Huang. Qoe-driven energy-aware multipath content delivery approach for mpt cp-based mobile phones. *China Communications*, 14(2):90–103, February 2017.

[6] Y. Chen, Y. Shen, J. Zhu, X. Jiang, and H. Tokuda. On the throughput capacity study for aloha mobile ad hoc networks. *IEEE Transactions on Communications*, 64(4):1646–1659, April 2016.

[7] M. M. Ghonge, P. M. Jawandhiya, and V. M. Thakare. Reputation and trust based selfish node detection system in manets. In *Proc. of the 2nd International Conference on Inventive Systems and Control (ICISC'18), Coimbatore, India*, pages 661–667. IEEE, January 2018.

[8] D. Hurley-Smith, J. Wetherall, and A. Adekunle. Superman: security using pre-existing routing for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 16(10):2927–2940, October 2017.

[9] R. Ji, Y. Cao, X. Fan, Y. Jiang, G. Lei, and Y. Ma. Multipath tcp-based iot communication evaluation: From the perspective of multipath management with machine learning. *Sensors*, 20(22):6573, November 2020.

[10] V. Kulathumani, A. Arora, M. Sridharan, K. Parker, and B. Lemon. On the repair time scaling wall for manets. *IEEE Communications Letters*, 20(8):1623–1626, August 2016.

[11] N. Kumai, R. Kumar, and R. Bajaj. Mobile ad hoc networks and energy efficiency using directional antennas: A review. In *Proc. of the 2017 International Conference on Intelligent Computing and Control Systems (ICICCS'17), Madurai, India*, pages 1213–1219. IEEE, June 2017.

[12] L. Li, J. Wang, X. Tao, C. Gu, and L. Wu. Local mobility perceptual model based on fuzzy logic in manet. *Research Briefs on Information & Communication Technology Evolution (ReBICTE)*, 5, November 2019.

[13] R. M, V. K, and S. T.S.B. Stable route aodv routing protocol for mobile wireless sensor networks. In *Proc. of the 2015 International Conference on Computing and Network Communications (CoCoNet'15), Trivandrum, India*, pages 917–923. IEEE, December 2015.

[14] S. Mhatre, H. Patil, and S. Kadam. Performance analysis of prediction and priority based routing protocol for manet's. In *Proc. of the 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI'17), Chennai, India*, pages 2911–2914. IEEE, September 2017.

[15] B. Ravi, K. K. Patil, U. K. K. Shenoy, and B. A. Holla. A simulation study of impact of low and high mobility on manet routing protocols. In *Proc. of the 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS'17),Chennai, India*, pages 1423–1428. IEEE, August 2017.

[16] A. K. Sharma, D. C. Noida, and A. Mishra. A study of energy optimization for manet. In *Proc. of the 6th International Conference on Computing for Sustainable Global Development (INDIACom'19),New Delhi, India, India*, pages 264–267. IEEE, March 2019.

[17] V. Sharma, I. You, F.-Y. Leu, and M. Atiquzzaman. Secure and efficient protocol for fast handover in 5g mobile xhaul networks. *Journal of Network and Computer Applications*, 102:38–57, January 2018.

[18] S. Shin and T. Kwon. Cryptanalysis of the anonymous authentication with key agreement scheme in wireless sensor networks. *Research Briefs on Information & Communication Technology Evolution (ReBICTE)*, 4, August 2018.

[19] R. Sun, J. Yuan, I. You, X. Shan, and Y. Ren. Energy-aware weighted graph based dynamic topology control algorithm. *Simulation Modelling Practice and Theory*, 19(8):1773–1781, September 2011.

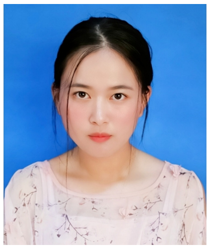
[20] Q. Ye and W. Zhuang. Distributed and adaptive medium access control for internet-of-things-enabled mobile networks. *IEEE Internet of Things Journal*, 4(2):446–460, April 2017.

Author Biography

Lejun Ji received a bachelor's degree in information management and information system from Liaocheng University in 2020, and is currently a master's degree in management science and engineering of Jiangxi Normal University.Her research interests include the next generation network transport protocols and network security management.

Gang Lei is currently the Dean, associate professor and master tutor of Software College of Jiangxi Normal University. His research fields are data mining, machine learning and computer linguistics. He has presided over or participated in more than 20 projects, published more than 20 academic papers and obtained 4 national software copyrights.

Ruiwen Ji received a bachelor's degree in engineering management from Beijing University of Posts and telecommunications in 2020, and is currently a master's degree in management science and engineering of Jiangxi Normal University.Her research interests include multimedia networks, Internet technology, information management and information systems.



Mengshuang Bao is currently studying software engineering (mobile terminal software development) in Jiangxi Normal University.Her research interests include the next generation network transport protocols and streaming media communication.

Hao Liu is currently studying software engineering (mobile terminal software development) in Jiangxi Normal University.His research interests include the next generation network transmission protocol and blockchain technology.

Zhuojun Dong is currently studying software engineering (mobile terminal software development) in Jiangxi Normal University.Her research interests include the next generation network transport protocols and streaming media communication.