ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

A SECURED AND RELIABLE ROUTING IN OPPORTUNISTIC NETWORK IN MANET USING TRUST MANAGEMENT SCHEME BASED ON BEHAVIOR FEEDBACK

Harish H S*, R Vijayan
M.Tech IT (Networking), VIT University, Vellore, India.
Asst Professor(SG), SITE, VIT University, Vellore, India.
Email: harryhs001@gmail.com

Received on 12-05-2016 *Accepted on 05-06-2016*

Abstract

In an uneven environment the movement of the nodes will be slow enough that they cannot utilize the opportunities effectively to know about the identity authentications in a self-organised network, and joining the network routing is also not possible. But what happens in opportunistic network is most of the communications takes place just by forwarding operations, so mutual authentication concept in minimal preference for each conversation. A trust based management scheme is presented here makes use of behaviour feedback where identity authentication is complemented. By making use of social attributes a certificate chains are formed, it is called as a local certificate graphs, mobile nodes make use of it to form a web of "Identity Trust" relationship. One more relationship called "behavior Trust" is established for nodes which moves slowly by making use of Verified Feedback Packets(VFP) generated by successors node based on positive behaviour of each node. Implementation of our trust scheme shows that the delivery probability and trust reconstruction ratio is improved effectively when network show up a large number of undesired nodes. If any nodes are attacked by any outsider our scheme will detect it and form alternative routing path. Our scheme also provides symmetric encryption for important messages to secure by attacker and also to overcome the complexity of asymmetric encryption.

Keywords: Opportunistic network, VFP, identity trust, behavior trust, forwarding algorithm, trust management scheme.

1. Introduction

As in the opportunistic network [1], there will be no central authority to identify the authentication of each node, a certificate chains are used. Chains are forms based on social attributes, nodes form the local certificate graphs to realise about the "identity trust" relationship. "Behavior trust" relationship is obtained by gathering the VFP's

generated by the successors. Trust is characterized as the certainty of a node that another node will execute not surprisingly [2]. A righteous trust relationship empowers a node to foresee and assess the association security to keep itself from being assaulted before the communication really happen. In the event that a node is continually ready to forward the got information packets, it will be viewed as reliable and holds a decent notoriety, where, as a result, its solicitations will be more conceivable to be fulfilled[7].

In view of the characteristics, for instance, openness and component topology, unrehearsed frameworks encounter the evil impacts of various attacks in data plane [3]. A great deal more appalling, a couple attacks can subvert or evade the once in a while used identity based security instruments. An achievable trust component amassing approach to manage ensure the trust organization system is impeccable with other security primitives, for instance, encryption and encapsulation [9].

Trust organization structure by fusing it into the improved association state directing (OLSR) tradition [5]. Unattended Wireless Sensor Networks (UWSNs) are depicted by long extends of isolated operation and settled or irregular intervals between sink visits [4]. The nonappearance of an online trusted third party recommends that present WSN trust organization arrangements are not fitting to UWSNs. A trust organization arrangement for UWSNs to give compelling and solid trust data storage and trust period.

2. Related work

In normal wireless networks, the nodes will get certificates from a certificate authorities or by any third party to communicate with other nodes safely. Nodes can also transfer its public keys through the trusted third party. Here it is called as a Cryptography based security scheme. But as in opportunistic networks nodes will moving frequently, so can't go for any authorities or third party.

The another scheme is Non-Cryptography based security scheme where often utilize the trust model or the reputation system to protect the data forwarding in opportunistic networks. As the security issue the nodes will be entering into network frequently, so it is necessary to get to know about the attackers who tries to attack the nodes. As in the opportunistic networks, the frequency of moving of nodes are high. So to form the best and efficient path to forward the data, and to secure the data is more important.

The transfer of keys or certificates between the nodes are vital as the network don't have any authorities to get the keys from. Trust is main issue in opportunistic networks to forward the data, by using the trust the key exchange can be achieved. Asymmetric key exchange algorithm is bit overhead as it includes two keys to securely transfer the data.

3. Proposed Trust management scheme

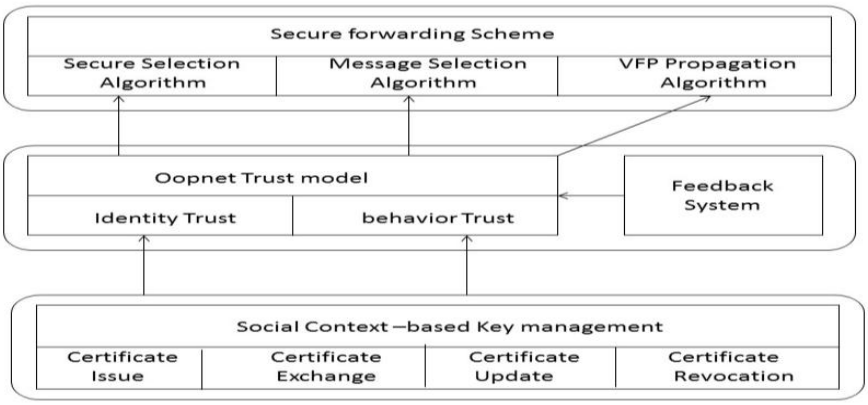

Fig 1 Proposed trust management architecture.

The scheme comes with three modules, context-based key management, trust model with feedback and secure forwarding. The certificate between each node are exchanged and organise themselves by making use of social-context information. But the main issue here is most of the honest nodes which comes in and goes out of the network can't participate in forwarding process, so it may reduce the performance. And also in opportunistic network the main operation in communication is just a forwarding operation, the need of complete establishment of identity authentications can be minimized.

The trust model is main part which takes care of gaining the trust between the nodes. The trust between nodes can be divided into "identity trust" and "behaviour trust". Making use of feedback information produced by other nodes, which is obtained by verified feedback packet, the security in enhanced and it also provides the reliability value for each nodes node can be analysed. The secure forwarding looks after how to send the data to the destination through an efficient and secured path. If the selected path is compromised, then trust model looks into another best path for forwarding.

3.1 Social context-based key management

The Social Context-Based management manages the issue of certificate, exchanging the certificates between the neighbouring nodes, and it also takes care of updating and revocation of certificates.

The following process will take place in this module.

- Nodes will find out their neighbors.
- The route request message is send.
- The route reply is send by the destination.
- The source node will issue the certificate.

3.2 Trust model

Identity trust

In opportunistic network, the certificate issues between all the nodes are not so efficient as in non-mobility network. It will be an overhead if nodes are moving in and out of the network frequently. As the forwarding the packets are the main criteria in opportunistic network, obtaining the trust of the neighboring nodes is enough. The trust can be obtained with the use of social attributes.

First the social attributes of the neighboring nodes are compared with the nodes own social attributes, if the similarity is more than the threshold value then it gains the identity trust of that neighboring node. It is just as example like, if a person A interacts with person B consistently, then it can be believed that sending message from person A to person B can be trusted. Some of the social attributes which can be looked into are:

- Energy level
- Frequency of forwarding messages
- The neighboring nodes it is interacting with

Behavior trust

The behavior trust plays an important role when 'identity trust' cannot be trusted fully. It can be obtained by the successor nodes while forwarding the message. Means by the feedback of the successor node.

As the node B gets a message from the node A, it looks for any misbehavior from the node A. If node B doesn't find any fault, it sends a positive feedback to its ancestor node. So here it can be said that node A is a trusted node and the counter value for is incremented by 1, if it not means the value will be decreased by 1. The trust model in the network looks into these values time by time or in the case if any attacker tries to attack the node. Actually this model will take care of the behavior trust relationship between nodes.

3.3 Secure Forwarding

Forwarding the message in an opportunistic network is done making use of the following algorithms.

- Successor selection
- Message selection
- VFP propagation algorithm

By using above three algorithms the secure forwarding of messages can take place. First the successor nodes to transfer the messages will be gathered, and trusted path will be selected in message selection to forward the message

securely. Third algorithm is used to generate the verified feedback packets to obtain the 'behavior trust' among the nodes.

3.3.1 Parameters used in Algorithm

1. X_a: mobile node
2. $S_{k:}$ the secret key
3. $C_{a,b}$: certificate from a to b
4. M: message to be transferred
5. Th_a: threshold of node a
6. $V_{a,b}$: verified feedback packet
7. $Tc_{a,b:}$ node a holds trust for node b
8. ID_i: identity number of node
9. $Y_{x:}$ trust model
10. Tc: trust counter

3.3.2 Successor selection

a. Message M is forwarded by node X_a to node X_b by using social attributes.

b. DO

c. X_b finds the X_c in its certified graph

d. if present

forward the message M to X_c

e. else if $Tc_{b,c}>Th_b$

f. then

Forwards the message to X_c

g. Else

h. Stores the message till proper node is obtained

3.3.3 Message selection

a. When X_c receive forwarding request of M from X_b

b. **If** X_c can find a valid $C_{c,b}$ or $Tc_{c,b} \geq Th_c$

c. **then**

X_c stores and carries M hoping to encounter another proper node.

d. **Else if** X_c can find a valid $C_{c,S}$, and the validity of M can be testified **then**

X_c stores and carries hoping to encounter another proper node.

e. **Else if** X_c can find a valid $C_{c,D}$

f. **then**

X_c temporarily holds M for a certain period.

g. **If** X_c can get obtain a valid $C_{c,b}$ or $C_{c,S}$ in certain period after several certificate graph exchanging

h. **then**

X_c stores and carries M hoping to encounter another proper node.

i. **Else** X_c drop M.

j. **End if**

k. **Else** X_c rejects the related forwarding request from X_b

l. End if

3.3.4 VFP propagation algorithm

a. For each and every node X_i

b. Do

c. If node Xj receives the message from previous node $X_{i,}$ it accepts the message as it in above algorithm

d. Then

X_j will sends a positive feedback by generating the packet $VFP_{j,i.}$

e. End if

f. End for

g. While trust model Y_x receives a $VFP_{j,i}$

h. Do

Y_x checks the validity by using the secret key

If valid

i. Then

Trust counter Tc is incremented by 1

j. End if

k. Else Tc remains same

l. End while

4. Simulation results and comparison

The system shows drastic improvement towards the existing system.

Here the trust management reconstruction ratio, packet drop ratio and the packet delivery are compared with the existing system and it shows a variable improvement by using the proposed system.

5.1 Trust reconstruction

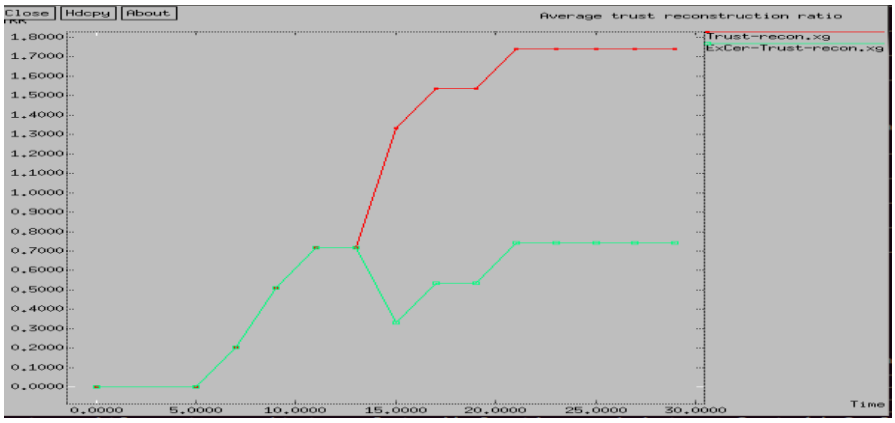

Fig 2: Graph for trust reconstruction.

Reconstruction of the routing path when the nodes are affected in the network are compared with existing non trust based system. The result shows that the average ratio of reconstructing the routing is higher than the normal system.

4.1 Packet delivery ratio

Packet delivery ratio is the main concern in networks. The prosed system shows a drastic improvement in the packet delivery time when compared to the existing system. It is because in normal system once the route is found out to be compromised, the detection and rerouting process takes a lot of time. And in normal conditions since the forwarding the message is main concern obtain the ‘identity trust’ is faster than the other all cryptography techniques.

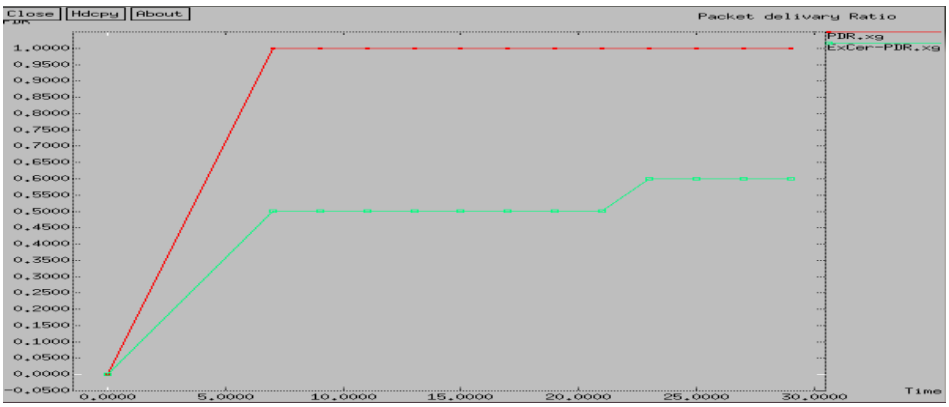

Fig 3: Packet delivery ratio.

4.2 Packet drop ratio

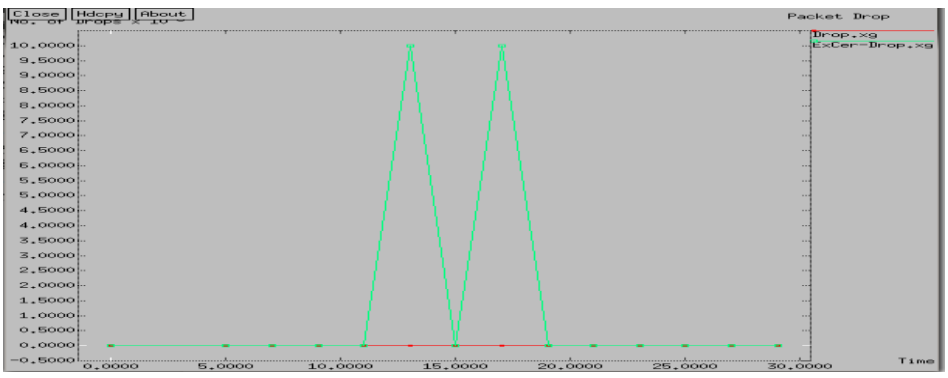

Fig 4: Packet drop comparison.

The above figure shows that there will be no packet drop in the proposed system. This is because as in the opportunistic forwarding pattern is 'storage-carry-forward', when the attacker comes and attacks the node, the node which are safe and participating in forwarding process just stores the message in its queue. So once the new path is identified the node will transfer the data which is stores, so there won't be any packet drops here.

5. Conclusion

Customary cryptography plan can just give the legitimate validation to mobile nodes characters, yet can't quantify the re-risk of nodes behavior. To take care of above issues, a novel trust administration plan in view of conduct criticism is proposed to support sending conventions in amazingly sparse opportunistic systems. The quick moving nodes understand the common character validation by using the declaration chains, and the "Identity Trust" relationship is developed in endorsement chart position. Then again, the successors create Verified Feed-back Packets for every positive criticism conduct to understand the common validation of sending message, and thus the "behavior Trust" relationship is framed. Hence, the difficult issue in validation for to a great degree sparse pioneering systems is explained, as "behavior Trust" can helps "identity Trust" to set up a more viable web of trust. Moreover, the safe sending convention which executes our trust plan can give higher system execution.

References

1. C Xi, S Liang, M Jianfeng, MA Zhuo "A trust management scheme based on behavior feedback for opportunistic networks" Communications, China, 2015 ieeexplore.ieee.org, Volume:12, issue:4 Page(s):117 – 129, Year-2015.
2. Renjian Feng, Xiaona Han, Qiang Liu, and Ning Yu "A Credible Bayesian-Based Trust Management Scheme for Wireless Sensor Networks" International Journal of Distributed Sensor Networks, Volume 2015 (2015), 9 pages, Year-2015.
3. S. Tan; X. Li, Q. Dong "A Trust Management System for Securing Data Plane of Ad Hoc Networks" IEEE Transactions on Vehicular Technology, Volume: PP, Issue: 99,Pages: 1 – 1. Year-2015.
4. Y. Ren; V. I. Zadorozhny, V. A. Oleshchuk; F. Y. Li "A Novel Approach to Trust Management in Unattended Wireless Sensor Networks" IEEE Transactions on Mobile Computing, Volume:13, Issue: 7 Pages: 1409-1423, IEEE Journals & Magazines, Year-2014.
5. N. Poolsappasit, M. Busby, S. K. Madria "Trust Management of Encrypted Data Aggregation in a Sensor Network Environment" 2012 IEEE 13th International Conference on Mobile Data Management Pages: 157-166, Year-2012.

6. Z. Su. L. Liu, M. Li, X. Fan, Y. Zhou "ServiceTrust: Trust Management in Service Provision Networks" Services Computing (SCC), 2013 IEEE International Conference on Pages: 272 - 279, Year-2013.
7. Xu Wu "A distributed trust model for mobile computing environments" Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on Year: 2010, Volume: 1 Pages: 248-252, IEEE Conference Publications, Year-2010.
8. Deepa S, Supriya M ,"Trust management schemes for intrusion detection systems -a survey", International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-2, Issue-8, Aug.-2014.
9. B. Poonguzharselvi and V. Vetriselvi, Ttrust framework for data forwarding in opportunistic networks using mobile traces", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 6, December 2012.
10. Er. Maggi Goyal, Er. Manoj Chaudhary, "Ensuring Privacy in opportunistic Network", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: Volume 13, Issue 2, PP 74-82, jul - aug 2013.
11. Shilpa N, Dr. S. Ambareesh, "Efficient Routing Protocol with Trust Management for Wireless Sensor Network", International Journal of Emerging Technology and Advanced Engineering, Volume 5, Special Issue 2, International Conference on Advances in Computer and Communication Engineering (ACCE-2015), may 2015.
12. Conti M, Giordano S, May M, et al. From opportunistic networks to opportunistic computing. Communications Magazine, IEEE, Vol 48, PP 126-139, Year-2010.

Corresponding Author:
Harish H S*,
Email: *harryhs001@gmail.com*