International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 7
ISSN: 2454-4248
41– 43

SAODV versus TAODV Technique using MANET routing Security

Ambresh Bhadrashetty
Assistant Professor,
Dept. of Studies in Computer Applications (MCA),
Visvesvaraya Technological University,
Centre for PG studies, Kalaburagi
ambresh.bhadrashetty@gmail.com

Gururaj S K
Student, MCA VI Semester,
Dept. of Studies in Computer Applications (MCA),
Visvesvaraya Technological University,
Centre for PG studies, Kalaburagi
gururaj555sk@gmail.com

Abstract **–**Recent technology SAODV (Secure ADHOC on Demand Distance Vector) ***uses*** Cryptography to send the data from one node to another. The problem with SAODV is, it is required to enter the 8-bit security key to send and receive data. If the number of present in the network are more, the SAODV protocol fails to deliver the data in time as the 8-bit security key has to be entered again and again. Therefore this demands a study where we are designing a Protocol TAODV in which all the nodes present in the network should get registered. The use of 8-bit security key is not required as in our study we are designing a Trusted Centre which provides security for the nodes connected to it.

*****

I. INTRODUCTION

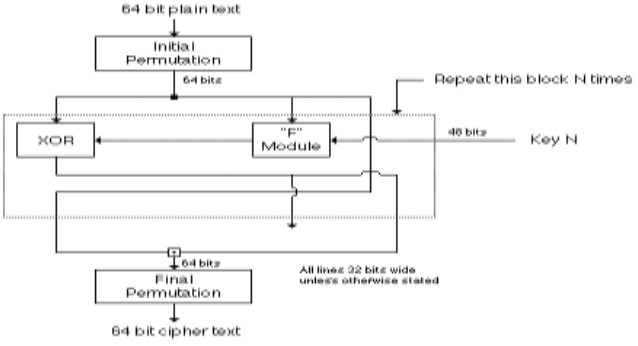
The SAODV uses the cryptographic methods where whenever the data is to be transferred we use 8-bit security key characters. While finding the node again the 8-bit security key charactersare to be entered which is a tedious task if the number of nodes are more. Once the route is found the receiver again has to use 8-bit security key characters to receive message. When we speak ofour proposed work that is TAODV here we are using a trusted center for the data transfer. The sender, route finder and receiver need not use any security key. As they should get registered to thetrusted center for the data transfer. The SAODV is not only a time consuming but it also increases the traffic in the networkwhere assume that there are some 6 nodes in the network namely Node#A, Node#B, Node#C, Node#D, Node#E and Node#F. Consider an example that Node#A wants to drive data to Node#F,once destination is known that is Node#F the very next thing what it does is to map the path first the request is sent to the nearest node that is Node#B there the 8-bit security key is to be authenticated, from Node#B to the next nearest node in the network and every new nearest node we have to authenticate it will the 8-bit security key. Once the route is found the sender can send the data again entering the 8-bit security key and the receiver after receiving the data has to use the same 8-bit security key to read the data or sent message. On the other hand we are aiming to design a protocol TAODV which does not require muchtime to transfer the data from one node to the other node that is destination. Here in the proposed work we are designing a protocol TAODV the following example explain the working of the new protocol. Assume there are six nodes in the network for the data communication. For the communication all the six nodes that is Node-A to Node-F should get registered to the trusted center. The trusted center is built upon encryption algorithms which helps the data to be securely transferredto the destinations without being leaked. And the proposed protocol does not take time which is taken by the previous protocol SAODV.

II. LITERATURE SURVEY

There were many studies conducted on the MANETS protocols. DES (Data EncryptionStandard) techniques were used for the design of the MANETS protocols. DES has a vital role inthe protocols standards for securing the data. Symmetric and Asymmetric algorithms weredesigned for the DES.

SAODV protocol was used for the data transmission to secure the data communicationbetween the nodes in the network. The problem with this protocol is that the use of security keyfor the data transmission has to be applied for finding the route, mapping the route and then sendingthe data to the receiver.

The DES algorithm was designed for 64-bit data key security but the problem with thisprotocol is that the use of 8-bit key security which has to be authenticated for finding the node inthe network for the data mapping of the route as well as transferring the data to thereceiver.



 ISSN: 2454-4248
41– 43

III. PROBLEM STATEMENT

The problem in the SAODV is that the protocol requires lot of time and the authorizationhas to be done to find the route, get the response by the neighbor node, and send the packets. TheSAODV protocol requires a three level authentication which should be disturbed across thenetwork from sender to the receiver. And it requires 8 key characters as password.

IV. METHODOLOGY

MANET routing protocols are very useful for the transfer of the data between the nodes.The source has a fixed path while communicating with the destination systems. These protocolsare largely dependent in the network for the better transformation of data between the nodes. Thewireless as well as the wired connection both uses these protocols.

ADHOC network on the other hand can be termed as a bench mark which has been designedfor one particular type of network. On the other hand there were many protocols designed for thedata transfer but some failed for security purpose and some for delay in the transmission.

Here we are aiming the present study to create a new protocol which can be used for thetransfer of the data between the nodes in the network and can also provide a better security whencompared whit the previous works.

We are designing a protocol TAODV where in which we are creating a trusted center whereall the nodes in the network has to get registered for the safe and secure communication. We areusing algorithms which are assuring that the nodes getting connected to the trusted center cancommunicate efficiently without any security issues.

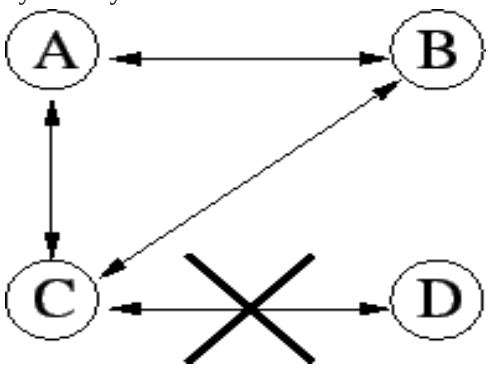
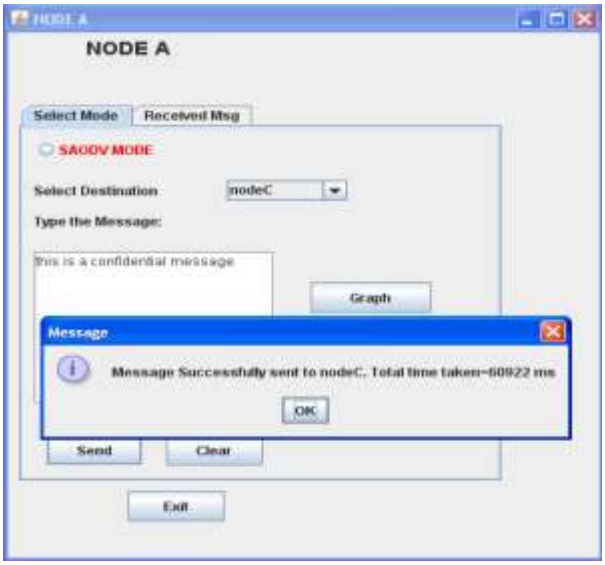
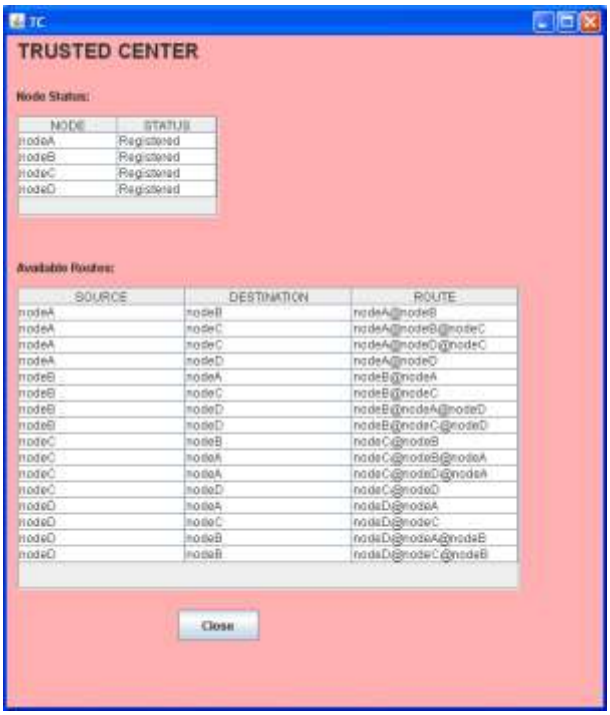


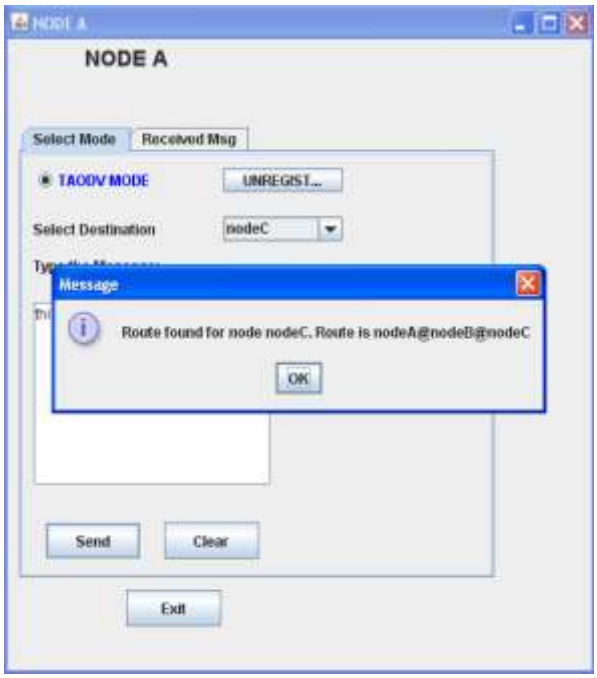
Fig. 1: "Counting 2 Infinity" problem

V. RESULTS





 ISSN: 2454-4248
41– 43



VI. CONCLUSION

In this paper we conclude that the SAODV protocol requires more time to find the route as when a new node is found it has the encrypt the data using the 8-bit security key which is a very tedious job if more nodes are present in the network. Apart from that the 8-bit security key has to be remembered all the time for the transmission of the data from source to the destination.

On the other hand TAODV is the best protocol for the data transfer in the ADHOC networks as in the TAODV we have created a Trusted-Center (TC) where all the nodes available in the network has to get registered for the safe and secure data transmission.

REFERENCES

[1] Martins, A, Faria, L., De Carvhalo, C., Carrapatoso, E.: User Modeling in Adaptive Hypermedia Educational Systems. In: Educational Technology & Society, vo. 11, n° 1,pp. 194_207(2008)

[2] Bellazi, R, Larizza, C., M., Milani, G., Nuzzo, A., Favalli, V., Arbustini, E: Translational ioinformatics: Challenges andOpportunities for Case-Based Reasoning and DecisionSupport. In: Case-Based Reasoning Research and Development,pp. 1-11(2010)

[3] El-Sappagh, S., El-Masri, S., Elmogy, M., Riad, A., Saddik, B.: An Ontological Case Base Engineering Methodology for Diabetes Management. In: Journal of medical systems, vol. 38, n° 8, pp. 1-14(2014)

[4] Isern, D., Moreno, A., Sanchez, D., Hajnal, A., Pedone, G., Varga, L.: Agent-based execution of personalized home care treatment. In: Applied Intelligence, vol. 34,n° 2,pp. 155-180(2011)

[5] Chen, H.,Compton,S.,Hsiao, O.: Daibetic Link:a health bid data system for patient empowerment and personalized healthcare. In:Smart Health,pp.71-83(2013)

[6] Huang, Z., Lu X., Duan, H., Zhao, C.: Collaboration-based medical knowledge recommendation In: Artificial intelligence in medicine, vol. 55,n° 1, pp. 13-24(2012)

[7] Yadav, N., Poellabaueuer, C.: An architecture for personalized health information retrieval. In: Proceedings of the 2012 international workshop on Smart health and wellbeing, pp. 41-48(2012)

[8] International Organization for Standarization: Ergonomics of human-system interaction _ Part 210: Human-centred design for interactive systems(2010)