Journal of Engineering and Applied Sciences 12 (Special Issue 2): 6240-6243, 2017
ISSN: 1816-949X

Efficient Improved Weakly Secure Network Segmentation using DKE

[1]Kirti Walia, [2]Vijay Dhir, [3]S.N. Panda and [4]Ashok Kumar
[1]IKGPTU, Jalandhar, Punjab, India
[2]Department of CSE, MK Group of Institutes, Amritsar, Punjab, India
[3]Chitkara University, Rajpura, Punjab, India
[4]DAV College, Ambala City, Haryana, India

Abstract: A lot of studies have been carried out to secure the network coding. Network coding can be defined as the transmission mode over any network. For a secure transmission a dynamic key is generated and these two are then mixed to secure the cipher text. These network coding are characterized into two groups: weakly secure shannon secure. The difference between these two groups is that weakly secure doesn't allow any outflow of meaningful information where as shannon secure didn't allow any kind of outflow of information. In this study, the security approach of improved secured network segmentation and dynamic key exchange has been blended, so as to reduce the attacks and threats to a network. It has also increased the efficiency of the network. We have also demonstrated the same in wireless sensor network scenarios under dynamic key exchange.

Key words: Shannon secure, weakly secure, network segmentation, improved secure network segmentation, network coding, transmission mode

INTRODUCTION

In the present day situation, we cannot expect anyone who is not in a network one way or the other. Security issues were incepted since the day two computers were connected to form a network. Also, since then firewalls are the first device to control the traffic and securing the networks (Walia *et al.*, 2013). When it comes to wireless networks, one have to be more cautious as the host systems become more vulnerable (Walia *et al.*, 2014). Now we can not imagine any kind of network environment like wired, wireless cloud and even ubiquitous computing without firewalls. Security is and will always remain the issue. Li *et al.* (2003) proved that with a restricted size field, one can achieve the highest flow of data from the single source to destination by linear network coding (Li *et al.*, 2003; Walia *et al.*, 2014; Koetter and Medard, 2003). On the basis of this network coding technology, network coding has confirmed its role not only in wired networks but also in wireless networks. Due to this network coding has to face a lot of security issues.

Bhattad and Narayanan suggested for a coding system called weakly secure. Further, working ahead on it, Silva and Kschischang (2009) suggested a common weakly secure network coding system. Jain (2004) planned a weakly secure network system using one-way function having limited eavesdroppers. Manuscript writers by Dong *et al.* (2008) and Mills *et al.* (2008) consider the security issues under various circumstances and other security necessities specifically in wireless sensor network. Researchers of the study (Du *et al.*, 2014) found that most of the researches had been done from the perspective of coding with given topologies and different coding algorithms were proposed in diverse network environments but they were unable to find any research in secure topology design. They also stated that by simplifying the topology design strategies a lot of memory and computing time can be saved. They restrict their study to the condition that the number of eavesdroppers are relatively few and under this condition they were able to reflect the advantage of topology design.

Literature review: Researchers of the study (Du *et al.*, 2014) combines the ISTD and SNS algorithm to integrate to form ISNS, a network segmentation and topology design. This resulted into an efficient algorithm. Total number of hubs, largest in-degree, rate of transmission and the likelihood of affected nodes in intermediate nodes were the parameters depending on which efficiency was evaluated. After comparing the two network design topologies they come to the conclusion that a lot of memory and computing time can be saved if linear network coding is considered.

As of late network (Du *et al.*, 2015; Ahlswede *et al.*, 2000) coding has pulled in noteworthy consideration in media transmission. The advantages of network coding to

Corresponding Author: Kirti Walia, IKGPTU, Jalandhar, Punjab, India

a correspondence network incorporate the expanded throughput and in addition secure information transmission. Reseachers have researched the benefits of applying network coding in sensor networks for security reason.

Specifically, the issue of building a protected unicast framework is considered. Not at all like past wiretapping situations where the danger is postured by outer wiretappers, security from an interior edge has been considered all hubs agree to the correspondence conventions yet are possible eavedroppers and the spies can collaborate with each other to decipher the packets sent from the originating hub. Not the same as most on hand research on network coding that outlines the network coding plan in view of a given topology, researchers had think about the network topology design. They initially attempt to discover the transmission topology that is reasonable for network coding in unicast framework. In light of the topology, they utilize straight network coding plan which is weakly secure. They direct recreations to demonstrate that it keeps agreeable eaves droppers from securing any helpful information transmitted from source to destination.

MATERIALS AND METHODS

Proposed work: In this study, we have developed and implemented a new algorithmic approach that makes use of the security in the ISNS algorithm. Using this approach, the secured key is generated at the source stage and is transmitted to the destination using AODV routing protocol. In the proposed approach, the secured key is mixed with a set of matrix that is having fake keys. By this method, the security is enhanced and the malicious node is not able to find the actual key.

Algorithmic approach:

- For the transmission of data node matrix is activated
- Node which start communication gets activated
- Source node generates the RREQ
- RREP by the next immediate nodes respond by RREP so that the path can be identified and generated
- For security reasons a dynamic key is generate
- To make the key more secure it is mixed with a set of fake keys
- To access the key attempts were made by the Malicious nodes
- Data packet follows the path which has already been generated
- The actual key is not been accessed by the Malicious nodes and failure attempts will be found
- If dynamic key gets matched this implies that it is a success and hence the packet will be handed over to the destination
- Otherwise it will be terminated because of authentication error or authentication failure because of dynamic key
- Go to step 1

Work flow:

- Generation of a dynamic graph based on the locations of wireless sensor nodes
- Implementation of the detection of malicious node in the network
- To highlight the malicious node in the network as early/prior detection of the attack
- Execution of the simulation in multiple iterations to get the transparent/non-biased results
- Comparison of results with the existing technique ISNS
- Implementation of the dynamic key exchange

RESULTS AND DISCUSSION

The proposed approach use hash based key that will traverse in the network intrusion can be avoided which will reduce the probability of threats and attacks. This dynamic key will be exchanged based on the key association in the list of existing keys. Further, the analysis of probability of the attack is done. We propose to secure the generated dynamic key by mingling it with forged keys. This mixing of keys reduces the chances of having access to the actual key which increases the security of the network.

The proposed algorithmic approach is implemented on wireless network scenarios for dynamic key exchange and accuracy as well the probability of finding out the fake or malicious node.

Success percent for the the proposed method and existing method: Table 1 depicts the 3 different simulation scenarios. On execution of the MATLAB code of 5 nodes, there is approx. The 96% accuracy or successful rate of avoidance of the malicious node. Similarly in case of 10 nodes, there is 90% accuracy of avoiding the malicious node.

Figure 1 depicts the scenario of different hubs. It is very much clear that the malicious hub (node 6) is separate from the network. In Fig. 2 when node 6 attempts to access the network by using its own created malicious key and is merged and connected with the network. Now at this point, node 6 will create its own dynamic key to access this network using own created malicious key (Fig. 3 and 4).

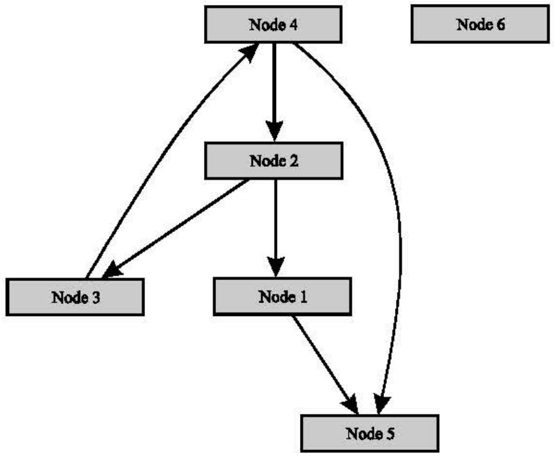

Fig. 1: Malicious hub neither detected or associated with the network

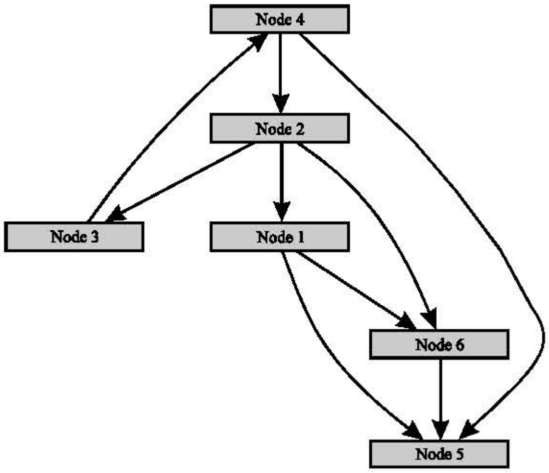

Fig. 2: Malicious hub gets associated with the network

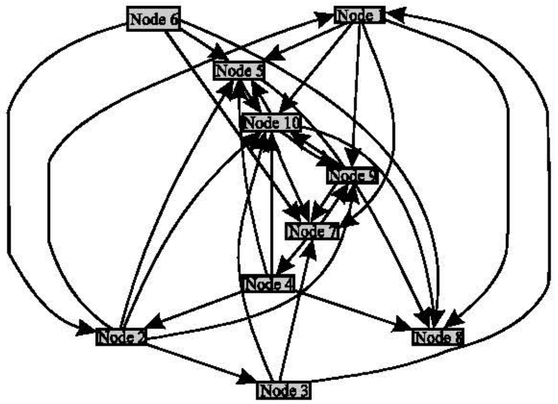

Fig. 3: Simulation scene when malicious nodes are associated with the network

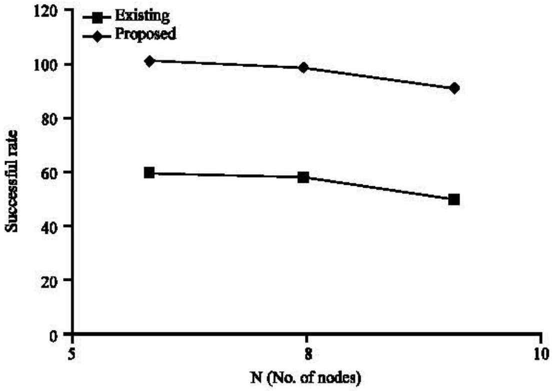

Fig. 4: Comparison between success percent and no. of hubs in existing and proposed method

Table 1: Success percent with total number of hubs (5, 8, 10) with proposed and existing method

Hubs/Methods	Proposed	Existing
5	8	10
89	89	95
49	57	59

CONCLUSION

The proposed approach is better wrt the classical approach as is evident from the results proved by the simulation of the proposed approach. Proposed method has been implemented and evaluates the security on the basis of dynamic key exchange. The proposed work keep the network more secured and in authentication mode with high security. This way not only the security but the integrity of the network is also enhanced. Further by the use of genetic algorithms proposed method can be improved and hence can be used in various other fields.

REFERENCES

Ahlswede, R., N. Cai, S.Y.R. Li and R.W. Yeung, 2000. Network information flow. IEEE Trans. Inform. Theory, 46: 1204-1216.

Dong, J., R. Curtmola, R. Sethi and C. Nita-Rotaru, 2008. Toward secure network coding in wireless networks: Threats and challenges. Proceedings of the 4th Workshop on Secure Network Protocols (NPSec 2008), October 19, 2008, IEEE, Orlando, Florida, USA. isBN:978-1-4244-2651-5, pp: 33-38.

Du, R., C. Zhao, F. Zhao and S. Li, 2015. Strategies of network coding against nodes conspiracy attack. Secur. Commun. Networks, 8: 2396-2403.

Du, R., C. Zhao, S. Li and J. Li, 2014. Efficient weakly secure network coding scheme against node conspiracy attack based on network segmentation. EURASIP. J. Wirel. Communi. Networking, 2014: 1-5.

Jain, K., 2004. Security based on network topology against the wiretapping attack. IEEE Wireless Commun., 11: 68-71.

Koetter, R. and M. Medard, 2003. An algebraic approach to network coding. IEEE/ACM Trans. Networking, 11: 782-796.

Li, S.Y.R., R.W. Yeung and N. Cai, 2003. Linear network coding. IEEE Trans. Inform. Theory, 49: 371-381.

Mills, A., B. Smith, T.C. Clancy, E. Soljanin and S. Vishwanath, 2008. On secure communication over wireless erasure networks. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2008), July 6-11, 2008, IEEE, Toronto, Ontario, Canada isBN:978-1-4244-2256-2, pp: 161-165.

Silva, D. and F.R. Kschischang, 2009. Universal weakly secure network coding. Proceedings of the IEEE Information Theory Workshop on Networking and Information Theory (ITW 2009), June 10-12, 2009, IEEE, Volos, Greece is BN:978-1-4244-4535-6, pp: 281-285.

Walia, K., S.N. Panda and H.C. Agrawal, 2013. A pragmatic analysis on software firewalls. Intl. J. Eng. Sci. Innovative Technol., 2: 574-578.

Walia, K., S.N. Panda and H.C. Agrawal, 2014. Effective architecture and algorithmic approach for secured firewall in sensor networks against assorted attacks. Intl. J. Multi Disciplinary Eng. Bus. Manage., 2: 36-41.