ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

A KEY DISTRIBUTION METHOD FOR PREVENTING MALICIOUS NODES IN MOBILE AD HOC NETWORK

Sowmiya.V[#1] , Valarmathi.S[#2]
[1]M.E. second Year CSE
Bharathiyar Institute of Engg for women. Salem,TamilNadu,India.
Sowmiyavenkat14@gmail.com
[2]Assistant Professor/CSE
Bharathiyar Institute of Engg for women. Salem,TamilNadu,India.
Valarit06@gmail.com

ABSTRACT

The Mobile ad-hoc networks (MANETs) are a network in which each mobile nodes voluntary cooperate in order to work properly. This cooperation among the nodes may increase the cost and some nodes in the network can refuse to cooperate, leading to the node misbehavior. Thus, the network performance will be seriously affected. These may have the limitations of high computational and communication overhead along with the lack of scalability and resilience to node compromise attacks. The Random key pre-distribution method is a scheme that is based on probabilistic key sharing among nodes within the sensor network. Key pre-distribution is the method of distribution of keys to the nodes before communication among the nodes. In some cases keys are randomly generated using a random number generator or pseudorandom number generator. Therefore, the nodes generate the network using their secret keys after implement that is when they reach their target position. The secret keys are generated, placed in sensor nodes and each sensor node searches the area in its communication distance to find another node to communicate.

Key words: Key distribution, secret keys, Pseudorandom generator

1. INRODUCTION

Mobile ad hoc network (MANET) is a regularly self-building, infrastructure-less network of mobile devices. Next-generation MANETs have to help a big range of data services. Data applications have basically varies transport aspect and varies service quality needs than old voice services, calling for important start from an old circuit switched work. In specific, the relative delay bearing of data applications, together with the split activity forms, lead to the possibility of scheduling movement so as to obtain efficiency improvement. An important attractive method, in fading environments, is to use channel-aware scheduling methods in

Enhanced protocol connected using the wires. "for this purpose" is a meaning for Ad hoc in Latin language. Every device in a MANET is freely to move individually in any direction and it will then modify its paths to other devices adequately. Each must transfer transport unrelated to itself use, and therefore it’s a router. The main challenge in building a MANET is equipping each device to regularly manage the information need to correctly route transport. Such networks may work by themselves or may be linked to the larger Internet. It may contain one or many and varies transceivers between nodes. This gives a highly dynamic, self topology.

MANETs are a nature of Wireless ad hoc network. Christo Ananth et al. [11] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.

2. EXISTING SYSTEM

In mobile ad hoc networks (MANETs), a basic need for the creation of communication among nodes is that nodes have to cooperate with one another. In the present of malicious nodes, this need will lead to severe security issues for example; such nodes may cause the routing process to be disrupted. In this concept, preventing or detecting misbehaving nodes will that create gray hole or combination black hole attacks are a problem. Here the concept make an effort to solve this problem by providing a dynamic source routing (DSR)-based routing technique, which is called as the cooperative bait detection scheme (CBDS), that combines the pros of both proactive and reactive defense methodology. The CBDS method uses a reverse tracing method to help in getting the above said goal. Simulation output are given, presenting that in the presence of misbehaving node attacks, the CBDS well performs the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in range of packet delivery ratio and routing problem.

3. PROPOSED SYSTEM

In the proposed approach RKP (Random Key Pre-distribution) is used .RKP methods have many varieties. The system operates by providing a key ring to each participating node in the sensor network before implementation. Key pre-distribution is the scheme of providing of keys onto nodes before deployment. Therefore, the nodes create the network with their secret keys after implementation, that is, when they reach their goal position. Secret keys are created and it is placed in sensor nodes and each sensor node finds the area in its conveying range to search another node to communicate. A secure path is created when two nodes find one or more common keys (this differs in each method) and communication is done on that link between those two nodes. Then the paths are established connecting these links, to create a connected graph. The result is a wireless communication network operating in its own way, according to the key pre-distribution scheme used in creation.

ADVANTAGES:

- Shared key scheme is used.
- Creation of path key.
- Each node distributes a key identifier list.
- Cancellation of a agreed node is very important in key distribution scheme.
- Separate privacy key each ring in network.

4. METHODOLOGY DESCRIPTION

4.1 Survey of Nodes:

The survey of nodes is used to find the details about nodes. The source nodes want to search the next transporting node, for sending data. Source node analyze, the next node is Secure or not. These modules analyze all the nodes in Wireless Sensor Network. Every node is analyzed in wireless sensor network. The secure node can be finding using this survey of nodes in the Wireless Sensor Network.

4.2 SET Protocol:

The Secure and Efficient data Transmission protocol for CWSNs (Cognitive Wireless Sensor Network). The RKP protocol is designed with the same purpose and scenarios for Cognitive Wireless Sensor Network with higher efficiency. The method introduces the concept of protocol initialization. The protocol initialization is introduced first and then it describes the key management of the protocol by using the RKP (Random Key Pre distribution) scheme, and the protocol operations afterwards.

The proposed method works similarly to the previous Key management, which has a protocol initialization prior to the network implementation and operates in rounds during communication.

4.3 Key management for security:

Key management for security is based on the DLP in the multiplicative group. The corresponding private pairing requirements are preloaded in the sensor nodes during the protocol introducing. Key storage and key update communication are two main categories in key management. Every device in a MANET is freely to move individually in any direction and it will then modify its paths to other devices adequately. So the key distribution has to be properly used to enhance the security. The key management uses encryption and decryption in the protocol to achieve secure data transmission, which has symmetric and asymmetric key based security.

4.4 Signing of signature:

Signing of signature is used for secure access and data transmission to nearby sensor nodes, by authorize with each other. Each node has each signature to authenticate the node, sender and receiver. And key is created for every data and sent to both receiver and the sender nodes. Signatures allow the user obtain neither the signature of a message in a way that the signer learns neither the message nor the resulting signature. RKP (Random Pre distribution) signature is used for this signature generation and key generation.

4.5 Verification:

The verification is implemented to verify whether the received message is valid or invalid. It checks whether the information is coming from secure sender and from the correct path. In case of any mismatch of keys between the nodes, the receiver won't allow the data to pass among the other nodes. After authentication, the receiver receives the information through the secure nodes.

5. ARCHITECTURE DIAGRAM

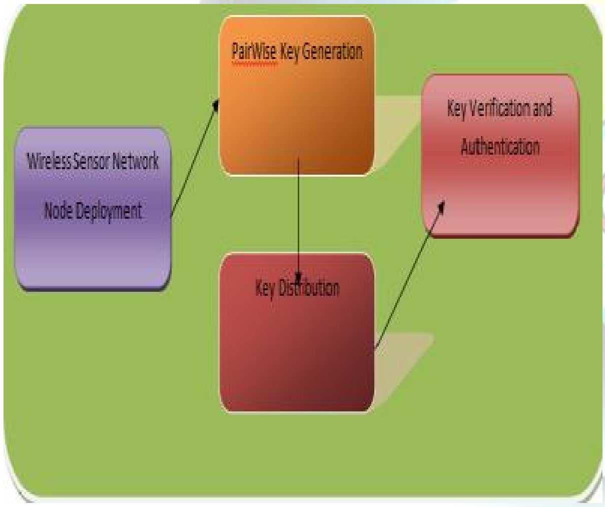
PairWise Key Generation
Wireless Sensor Network Node Deployment
Key Verification and Authentication
Key Distribution

Figure 5.1: Architecture of random key pre distribution method

Figure 5.1 explains the basic architecture of random key distribution method. In this method the source node have find the nodes that are secure enough to transfer the data throughout the communication to the destination node. First the source node will create the authenticated key and its signature. Then the key is passed through the path to the next intermediate nodes. Every node in the communication will have to create its own authenticated key for the secure transfer of data. If the source node finds the entire secure node then the secure link is established. The method introduces the concept of protocol initialization. An important attractive method, in fading environments, is to use channel-aware scheduling methods in Enhanced protocol connected using the wires. The nodes which are involved in communication should check the key in which it is receiving from the neighbor node. If the keys of the nodes in the link are matched between two nodes then the data is transferred among the two nodes. If the keys between two nodes are not matched then it can be found as malicious node.

CONCLUSION

The random key pre distribution method makes the message sender easy to defend against the misbehaving nodes in MANET environment. This method makes the use of key management which gives the efficient way of sending the message. The key will be distributed onto each node that is participating in receiving and delivering the message. The attacker may find it difficult to work against the key management because it follows key ring. The source node will find the next secure node to transmit the data. Therefore, the nodes create the network using their secret keys after implementation, that is, when they reach their destination position. Signing of data by the sender will create its own identity. Secret keys are created, placed in sensor nodes and each sensor node searches the area in its conveyable range to search another node to communicate. Key generation is the process of creating keys for cryptography. A key is used to encrypt and decrypt the data in spite of the data send. In some cases keys are randomly generated using a random number producer or pseudorandom number producer. Thus this random key pre distribution method securely transmits the data.

FUTURE WORK

In the future work, the key management can be enhanced for sending and receiving the data. Each node will create its own signature that is used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. The key is generated in the way in which it cannot be compromised by the attacker. The energy consumption which can be used to detect the malicious nodes will be reduced to greater amount. Also verification process is included to verify whether that the received data authenticated or not.

REFERENCES

[1] C. Chang, Y.Wang, and H. Chao, "An efficientMesh-based core multicast routing protocol onMANETs," *J. Internet Technol.*, vol. 8, no. 2, pp. 229–239, Apr. 2007.

[2] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.

[3] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in *Proc. IEEE Aerosp. Conf.*, 2002, vol. 6, pp. 2727–2740.

[4]A. Baadache and A.Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265.

[6] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," *Int. J. Comput. Appl.*, vol. 1, no. 22, pp. 28–32, 2010.

[7] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[8] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002.

[9]S.Ramaswamy,H.Fu,M.Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575.

[10] H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in *Proc. IEEE ICC*, 2007, pp. 362–367.

[11] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[12] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in *Proc. WiSec*, 2009, pp. 103–110.

[13] W. Wang, B. Bhargava, and M. Linderman,"Defending against collaborative

packet drop attacks on MANETs," in *Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst.*, New Delhi, India, Sep. 2009.

[14] QualNet Simulaton Tool, Scalable Network Technologies. (Last retrieved March 18, 2013). [Online]. Available: http://www.qualnet.com

[15] *IEEE Standard for Information Technology*, IEEE Std 802.11-14997,1997, Telecommunications and Information exchange between systems: wireless LAN medium access control (MAC) and physical layer (PHY)Specifications, pp. i-445.