International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 693 - 696, 2014, ISSN: 2319–8656

Hop- by- Hop Message Authentication and Wormhole Detection Mechanism in Wireless Sensor Network

S.Subha
Computer Science and Engineering
V.S.B Engineering College
Karur, India

U.Gowri Sankar
Computer Science And Engineering
V.S.B Engineering College
Karur, India

Abstract: One of the most effective way to prevent unauthorized and corrupted message from being forward in wireless sensor network. So to restrict these problems many authentication schemes have been developed based on symmetric key cryptosystem. But there is high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. So to address these isuues polynomial based scheme[1] was introduced. But in these methods it having the threshold problem that means to send the limited message only because to send larger number of message means the attacker can fully recover. So in my existing system a scalable message authentication scheme based on elliptic curve cryptography. This scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. But these method only detect the black hole and grey hole attacks are dected but does not detect the worm hole attack. In my proposed system to detect the worm hole attack. Worm hole attack is one of the harmful attack to which degrade the network performance. So, in the proposed system, one innovative technique is introduced which is called an efficient wormhole detection mechanism in the wireless sensor networks. In this method, considers the RTT between two successive nodes and those nodes' neighbor number which is needed to compare those values of other successive nodes. The identification of wormhole attacks is based on the two faces. The first consideration is that the transmission time between two wormhole attack affected nodes is considerable higher than that between two normal neighbor nodes. The second detection mechanism is based on the fact that by introducing new links into the network, the adversary increases the number of neighbors of the nodes within its radius. An experimental result shows that the proposed method achieves high network performance..

Keywords: **Hop-by-hop authentication, public-key cryptosystem, source privacy, Modified ELGamal signature, Round Trip Time.**

1. INTRODUCTION

A Wireless Sensor Network is a self-configuring network of small sensor nodes communicating among themselves using radio signals, and deployed in quantity to sense, monitor and understand the physical world.A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver, which can be hard-wired or wireless, receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from the electric utility or from a battery.

2. PREVIOUS WORK

A message authentication code [11] is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. So in wireless communication the message will be hacked by the attacker can modify message. So to avoid the attacker so many methods are introduced in wireless sensor networks. Many message authentication scheme have been developed. It have the limitation of high computational and communication overhead in addition to lack of scalability to node compromised attack. So to avoid this problem we introduce polynomial based scheme was introduce. But this algorithms also having some problem. While enabling intermediate node authentication[2]. When the number of message transmitted is lager then the threshold , the attacker can fully recover the polynomial. So to avoid this problem in my existing system to introduce Modified Elgamal Signature[4] scheme was developed this is used for signature verification process. Then another method was also implemented that is SAMA on elliptic curve these is used in verification process. This scheme allows any node to transmit an unlimited number of message without suffering the threshold problem. This method also detect the block hole and gray hole attack.

DRAWBACK OF EXISTING SYSTEM

1. This method does not detect the wormhole attack.
2. Degrade the network performance.
3. It does not have computational and communication overhead.
4. It have less efficiency.

3. TERMINOLOGY AND PRELIMINORY

3.1 Model And Assumption

Security is an important concern in the wireless sensor networks. Message authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. In addition to that, in the wireless sensor networks, wormhole attacks can cause severe damage to the route discovery mechanism used in many routing protocols. In a wormhole attack, the malicious nodes will tunnel the eavesdropped packets to a remote position in the network and retransmit them to generate fake neighbor connections, thus spoiling the

routing protocols and weakening some security enhancements.

3.2 Terminology

i. Modified ElGamal Signature Scheme

The modified elgamal signature [5] scheme consist of three algorithms:

Key generation algorithm. Let p be a large prime and g be a generator of $\mathbb{Z}$: Both p and g are made public. For a random private key^{p} x 2 $\mathbb{Z}_p$, the public key y is computed from y ¼ g^x mod p.

Signature algorithm. The MES can also have many variants. For the purpose of efficiency, we will describe the variant, called optimal scheme. To sign a message m, one chooses a random KϵZ^*_{p-1},then computes the exponentiation r=g^k mod p.

Verification algorithm. The verifier checks whether the signature equation g^S ¼ $ry^{rh\eth m;r\flat}$ mod p: If the equality holds true, then the verifier Accepts the signature, and rejects otherwise.

4. PROPOSED WORK

In my existing system to detect the black hole and gray hole attack. But does not detect the wormhole attack[9]. So one innovative techniques is used in my proposed work which is called on efficient wormhole detection mechanism in wireless sensor network.

Definition: In this section, to detect the wormhole attack which is based on the RTT of the message between successive nodes and their neighbor numbers.So we finding wormhole attack by using two mechnisums:

1. **Route Finding**: At that phase, the source node is responsible to construct the hierarchical routing tree to other nodes in the sensor field. The node sends the route request (R_{REQ}) message to the neighbor node and save the time of its R_{REQ} sending T_{REQ}. The intermediate node also forward the R_{REQ} message and save T_{REQ} of its sending time. When the R_{REQ} message reach to the destination node, it reply route reply message (R_{REP}) with the reserved path. When the intermediate node receives the R_{REP} message, it saves the time of receiving of R_{REP} T_{REP}. Our assumption is based on the RTT of the route request and reply. The RTT can be calculated as

$$\mathbf{RTT = T_{REP}-T_{REQ}}$$

All intermediate nodes save this information and then send it also to the base station.

2.Construction of neighbor list: In this first phase, each node broadcast the neighbor request (N_{REQ}) message. The N_{REQ} receiving node responds to the neighbor reply (N_{REP}) message. The requesting node constructs the neighbor lists based on the received of N_{REP} messages and counts its neighbor number (*nn*). After that the source node starts the route construction phase.

ADVANTAGE OF PROPOSED WORK

1. To detect the wormhole detection
2. It give high network performance
3. This method having high efficiency
4. It give high message source privacy.

5. RELATED WORK

In my existing system secret polynomial-based message authentication scheme was introduced. This sharing scheme, where the number of message transmition is below the threshold means system will be secure and the enables the intermediate to node to verify the authenticity of message. But the message is large than the threshold means the system should be compromised by the attacker, then system should be completely broken. Then to avoid these threshold problem to introduce Modified ELGamal[5] Signature scheme which is used in my existing system. While enabling intermediate node authentication allows any node to transmit unlimited number of message without suffering the threshold problem. Then the system should be in very secure and attacker does not compromise the nodes. Then these type of MES schemes also to find the block hole and gray hole attack. But this method does not detect worm hole attack because worm hole attack is one harm full attack which degrade the network performance.

So in my proposed system to find the wormhole attack by using the RTT between two successive nodes. Then worm hole attack is a malicious node tunnels message received in one part of the network over a low latency link and replay them in a different part. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.

6. PROPOSED WORMHOLE DETECTION MECHANISUM

In this section we present our wormhole detection[9] mechanism. Our detection is based on the RTT of the message between nodes.

System modules: These wormhole detection mechanism using some method to detect the attacker that's are:

1. Route Finding
2. **Construction of neighbor list**
3. **Wormhole Attack Detection**
4. **Calculation of RTT**
5.

Phase1: Route Finding

At that phase, the source node is responsible to construct the hierarchical routing tree to other nodes in the sensor field. The node sends the route request (R_{REQ}) message to the neighbor node and save the time of its R_{REQ} sending T_{REQ}. The intermediate node also forward the R_{REQ} message and save T_{REQ} of its sending time. When the R_{REQ} message reach to the destination node, it reply route reply message (R_{REP}) with the reserved path. When the intermediate node receives the R_{REP} message, it saves the time of receiving of R_{REP} T_{REP}. Our assumption is based on the RTT of the route request and reply. The RTT can be calculated as

$$RTT = T_{REP} - T_{REQ}$$

All intermediate nodes save this information and then send it also to the base station.

Phase2: **Construction of neighbor list**

In this first phase, each node broadcast the neighbor request [11] (N_{REQ}) message. The N_{REQ} receiving node responds to the neighbor reply (N_{REP}) message.The requesting node constructs the neighbor lists based on the received of N_{REP} messages and counts its neighbor number (nn). After that the source node starts the route construction phase.

Phase3: Wormhole Attack Detection

In this phase, the source node calculates the RTT [9] of all intermediate nodes and also it and destination. It calculates the RTT of successive nodes and compares the value to check whether the wormhole attack can be there or not. If there is no attack, the values of them are nearly the same. If the RTT value is higher than other successive nodes, it can be suspected as wormhole attack between this link. The nextdetection mechanism is based on the fact that by introducing new links into the network graph, the adversary increases the number of neighbors of the nodes within its radius. So it needs to check the nn of these two nodes which find in section 4.2. Equation (2) is adopted form [5] to estimate average number of neighbors d. It is approximated as

$$d = (N-1)\,\pi\, r^2 / A$$

where A is the area of the region, N is the number of nodes in that region and r is the common transmission radius. For example, if the RTT value between A to B is considerably greater than for other links, it needs to check the value of nn for A and B. If also the nn value for A and B is higher than the average neighbor number d, there is a suspect that a wormhole link is between nodes A and B. In this way the mechanism can pin point the location of the wormhole attack.

Phase 4: Calculation of RTT

In this subsection, the detailed calculation of the RTT is discussed. The value of RTT is considered the time difference between a node receives R_{REP} from a destination to it send R_{REQ} to the destination. During route setup procedure, the time of sending R_{REQ} and receiving R_{REP} is described in Figure 1. In this case, every node will save the time they forward R_{REQ} and the time they receive R_{REP} from the destination to calculate the RTT. Given all RTT values between nodes in the route and the destination, RTT between two successive nodes, say A and B, can be calculated as follows:

$$RTT_{A,B} = RTT_A - RTT_B$$

Where RTT_A is the RTT between node A and the destination, RTT_B is the RTT between node B and the destination. For example, the route from source (S) to destination (D) pass through node A, and B so which routing path includes:

$$S \rightarrow A \rightarrow B \rightarrow D$$

whereas $T(S)_{.}$, $T(A)_{REQ}$, $T(B)_{REQ}$, $T(D)_{REQ}$ is the time the node S, A, B, D forward R_{REQ} and $T(S)_{REP}$, $T(A)_{REP}$, $T(B)_{REP}$, T(D)REP is the time the node S, A, B, D forward REP. Then the RTT between S, A, B and D will be calculated based on equation as follows:

$$RTT_S = T(S)_{REP} - T(S)_{REQ}$$

$$RTT_A = T(A)_{REP} - T(A)_{REQ}$$

$$RTT_B = T(B)_{REP} - T(B)_{REQ}$$

$$RTT_D = T(D)_{REP} - T(D)_{REQ}$$

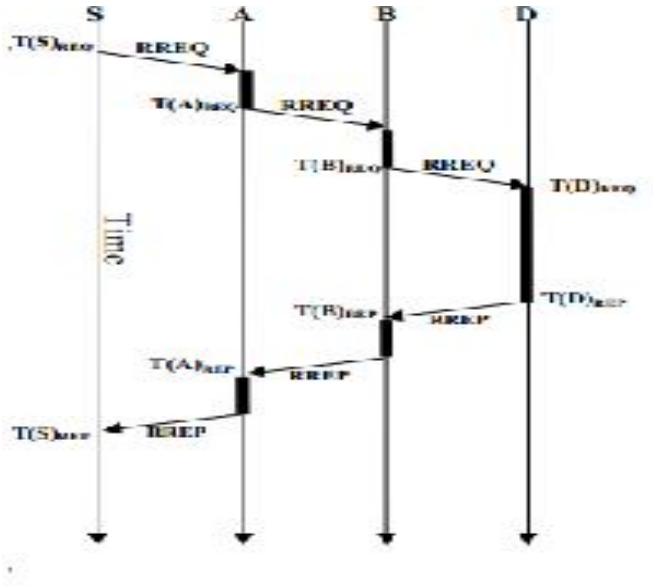
And the RTT values between two successive nodes along the path will be calculated based on equation :

$$RTT_{S,A} = RTT_S - RTT_A$$

$$RTT_{A,B} = RTT_A - RTT_B$$

$$RTT_{B,D} = RTT_B - RTT_D$$

Under normal circumstances, $RTT_{S,A}$, $RTT_{A,B}$, $RTT_{B,D}$ are similar value in range. If there is a wormhole line between two nodes, the RTT value may considerably higher than other successive RTT values and suspected that there may be a wormhole link between these two nodes.



7. CONCLUSION

In this paper, we first proposed a novel and efficient worm hole detection based on RTT. While ensuring message sender privacy. RTT can be applied to any message to provide message content authenticity and then node compromised attack. To provide hop by hop message authentication without the weakness of the build in block hole attack. We proposed hop by hop message authentication scheme based on RTT. When applied to the wireless sensor network with fixed number of sink nodes, we also discussed in possible

techniques for compromised node identification. We compare our proposed scheme with MES scheme through simulation using NS-2 simulator. The simulation results show that our system has acceptable range of performance and applicability. Both theoretical and simulation result shows that, in comparable scenario, our proposed scheme is more efficient then the MES scheme in terms of computational overhead, energy consumption, message delay and memory consumption.

8. REFERENCES

[1] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.

[2] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. Advances in Cryptology (Crypto '92), pp. 471-486, Apr. 1992.

[3] D. Chaum, "The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.

[4]T.A. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

[5] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," Proc. IEEE Symp. Security and Privacy, May 2000.

[6] D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT), pp. 387- 398, 1996.

[7] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Proposal for Terminology," http://dud.inf.tu-dresden.de/ literatur/Anon_Terminology_v0.31.pdf, Feb. 2008.

[8] [7] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[9] N. Song, L. Qian, and X. Li. Wormhole Attacks Detections in Wireless Ad Hoc Networks: A Statistical Analysis Approach. In Proceeding of the 19th International Parallel and Distributed Processing Symposium.

[10] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-By- Hop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[11] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.