Dynamic Window Based Multihop Authentication for WSN

Yao Lan
College of Information Science and Engineering,
Northeastern University
Shenyang, China
yaolan@mail.neu.edu.cn

Yu Zhiliang
College of Information Science and Engineering,
Northeastern University
Shenyang, China
yuzhiliang_007@163.com

Zhang Tie
College of Information Science and Engineering,
Northeastern University
Shenyang, China
adrianchen@live.cn

Gao Fuxiang
College of Information Science and Engineering,
Northeastern University
Shenyang, China
gaofuxiang@mail.neu.edu.cn

ABSTRACT

Per-hop authentication is the most effective way to prevent DOS attacks during multihop data delivery. Although the study results show that Public Key Cryptography (PKC) is feasible on sensor nodes with limited resources, it is still very expensive to perform per-hop authentication using public key digital signature. To solve the problem that the resources of WSN is exhausted quickly by PKC, Dynamic Window Based Multihop Authentication(DWMA) for WSN is proposed in this paper. Dynamic window makes it possible to pay only a small number of authentication based on digital signature for confining DoS attacks effectively in a small scope and locating suspicious nodes quickly. Experimental results show that DWMA could save more resources than per-hop authentication for WSN, defend DoS attacks effectively and locate malicious nodes. It's an effective protocol for ensuring the resistance of DoS in routing.

Categories and Subject Descriptors

H.4 INFORMATION SYSTEMS APPLICATIONS, H.4.3 Communications Applications

General Terms: Security

Keywords: DoS, dynamic window, multihop authentication

1. INTRODUCTION

The goal of DOS attacks in WSN is to keep the legitimate node from accessing the destination node. In WSN, DOS attacks could be divided into two types: positive attacks and passive attacks [1]. The best way of defending the positive DOS attacks is to verify the integrity, authenticity and freshness of messages via per-hop authentication. That could discover and discard suspicious messages immediately after anomalous messages are injected into WSN.

At present, there have been many message authentication schemes for different application environments, such as SNEP, TinySec, ZigBee, MiniSec, one-way hash chain, and LEDS, and so on [2,3,4,5,6]. These authentication algorithms mainly use one-way hash function or MAC to implement per-hop authentication, but their security and flexibility are not well. The digital signature based on public key is a better choice for message authentication compared with the above authentication algorithms, but many people think that its cost is very terrible and unrealistic for sensor nodes. The experiment shows that the cost of one ECDSA-160 sign and one ECDSA-160 authentication are 22.82mJ and 45.09mJ respectively, and PKC is feasible on sensor nodes [7]. Furthermore, the public key infrastructure has been implemented on the 8-bit, 7.3828-MHz MICA2 mote [8]. However if sensor nodes using EDCSA-160 authenticate every message, the resource consumption is still very expensive, especially in per-hop authentication.

In fact, most overhead of per-hop authentication occurs in normal messages, which is actually not essential. When digital signature based on public key is used to verify messages in multihop data delivery, if it is possible that DoS attacks could be limited without verifying normal messages, the resource consumption will be acceptable for WSN. To achieve the target, this paper proposes a novel scheme: dynamic window based multihop authentication (DWMA). The proposed scheme doesn't only avoid most of needless authentication for authentic messages, but also limit DOS attacks effectively, and could locate malicious nodes quickly. More importantly, the energy consumption of the proposed scheme using digital signature based on public key is no more than that of per-hop authentication using one-way hash function or MAC.

2. USING DYNAMIC WINDOW TO VERIFY MESSAGES DURING MUTIHOP DATA DELIVERY

2.1 System Model

In this paper, we assume that the attack objective is to consume nodes' limited resources and stop the delivery of normal data. To achieve the objective, the attacker would try to capture normal nodes or deploy malicious nodes. These anomalous nodes could tamper received messages, flood faked messages, and replay old messages. To confuse normal nodes, attackers may send anomalous messages randomly or with a certain probability.

We assume that the topology of WSN is static, and WSN will implement neighbor discovery mechanism to establish neighbor lists in every node. Nodes only communicate with nodes in their own neighbor lists. Meanwhile, attackers can't move any malicious nodes after starting to attack.

2.2 Design Targets

The goal of this paper is to verify messages via digital signature based on public key, defend the positive DOS attack and locate attack sources quickly. The design principles include:

CCS'10, October 4-8, 2010, Chicago, Illinois, USA.
ACM 978-1-4503-0244-9/10/10.

1) Effectiveness: DWMA should contain the damage of DOS attacks very well and find out malicious nodes quickly.

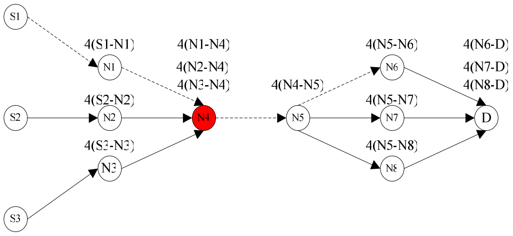
2) Savings: the message authentication using digital signature based on public key shouldn't consume too many resources and even consume less energy than per-hop authentication based on MAC or one-way hash chain in the long run.

3) Flexibility: DWMA should be able to be applied to kinds of WSN routing protocols.

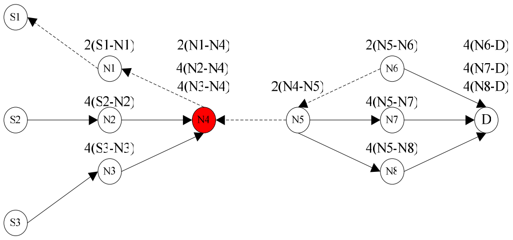
2.3 DWMA

DWMA is to improve the broadcast authentication mechanism based on dynamic window in [9]. In this scheme, every message adds a field da: it records the number of passed nodes after the last authentication. At the same time, every sensor node needs to maintain a neighbor table: sensor nodes set the corresponding window value W, the growth delay degree R_{delay} of W, and the history record B_{num} of anomalous messages for every neighbor node.

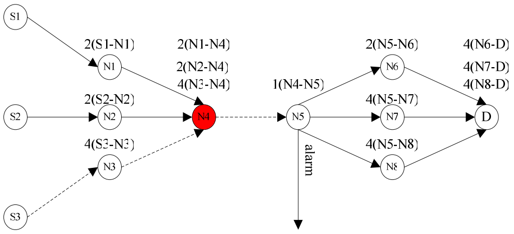
W controls the maximum number of nodes that forward the message M which isn't verified. Once the hop number da of M received by S is not less than the corresponding W, S must verify M. If authentication is successful, execute different functions by judging the value of R_{delay}: when $R_{delay} = 0$, this function ψ_s is executed; when $R_{delay} > 0$, the function R_m is executed. If authentication fails and W>1, the function ψ_m is executed. At this time, if R_{delay}=0, B_{num}= B_{num}+1, the update function R_u is executed. Finally, the window decreasing message DATA_W_REDUCE, which is to be forwarded d_a*-1* hops at most, is sent along the reverse path of data delivery. If authentication fails and W=1, S sends the alarm message DATA_W_ALARM to the last node, and warns the last node to send messages to it after verifying messages. The process of DWMA is shown in Fig.1.



(a)



(b)



(c)

Fig. 1 the sketch map of DWMA process

Shown in Fig.1(a), at first, the value of W_{max} is 4 for all nodes and W=W_{max}. S1 sends a message M to D. When N4 receives M, N4 tampers M and sends it to N5. Then N5 sends M to N6. N6 find that d_a >=$W_{(N5\text{-}N6)}$, and then verifies M. But the authentication fails and R_{delay}=0. So N6 executes these formulas for N5 in turn: B_{num}= B_{num}+1=1, R_{delay}=R_u=2^{Bnum}=2, $W_{(N5\text{-}N6)}$=ψ_m=$W_{(N5\text{-}N6)}$/2=2. Finally, N6 discards M, and forwards DATA_W_REDUCE along the reverse path of the M delivery path S1-N1-N4-N5-N6(shown in Fig.1(b)). When one of these nodes in the reverse path receives DATA_W_REDUCE, it executes those formulas that N6 has executed and forwards DATA_W_REDUCE to the next node in the reverse path. When N5 receives the second anomalous message from N4 again, $W_{(N4\text{-}N5)}$=1. As given in Fig.1(c), when N5 receives the third anomalous message form N4, N5 sends the alarm message DATA_W_ALARM to N4. If N4 continues to sends anomalous messages to N5, N5 sends the alarm message to the sink node and isolates N4.

3. ANALYSIS AND EVALUATION

In this chapter, DWMA is analyzed and evaluated using OMNET++4.0. The following performances are evaluated: 1, throughput (the amount of data received by the sink); 2, authentication times in WSN; 3, the total energy consumed in WSN.

3.1 Environmental Setup

In this simulation, we assume that we assume that sensor nodes run on the Berkeley/Crossbow Mica2dot sensor platform[7]. In the simulation environment, there are 100 uniformly deployed sensor nodes, ten of which are malicious nodes.

During the simulation, the initial value of W is W_{max}(100), the growth function of W is ψ_s=W+1, the decreasing function of W is ψ_m=W/2, the update function of R_{delay} is R_u=2^{Bnum}, and the decreasing function of Rdelay is Rm=R delay-2*W.

3.2 Simulation and Result Analysis

We simulate different DOS attacks varying in the ratio, in which malicious nodes tamper messages. The tampering ratio ranges from 0 to 100%. By default, DWMA uses public key based digital signatures to authenticate data, unless there are special instructions.

Fig.2 shows that the total energy consumption using DWMA after the source node S sends 2000 messages with the intensity of DOS attacks changing from 0 to 100%. As given in Fig.2, the per-hop authentication method using digital signature based on public key consumes too much energy compared with DWMA. We also notice that the energy consumption of DWMA is less than that of the per-hop authentication method based on MAC. Meanwhile, DWMA using MAC consumes less energy than the per-hop authentication method based on MAC, but the difference of their energy consumption is very small. The reason is that the energy is mainly consumed by the communication between nodes, the cost of authentication using MAC only makes up a small part of the total energy consumption. In the process of the simulation, the throughput achieves up to 85% in all different cases, and the possibility that malicious nodes are detected successfully is more than 90%. This is a clear indication that DWMA achieves nearly the same effect compared with the per-hop authentication but consumes less energy. Thus it is economical in energy consumption and robust against DOS attacks.

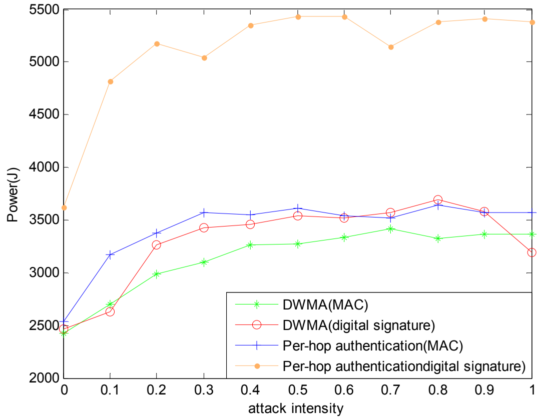


Fig. 2 the energy consumption in different intensity of DOS attacks

Malicious nodes could confuse authenticable nodes and increase authentication times by changing the hop number of messages. The result is shown in Fig.3.

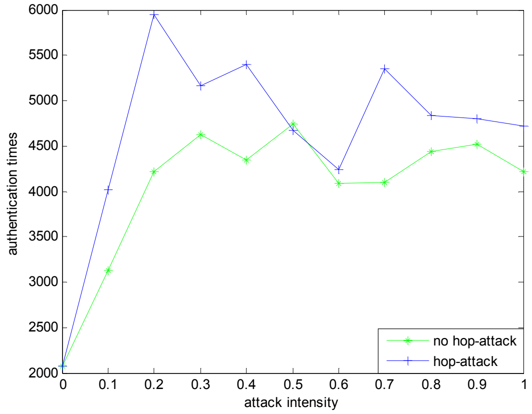


Fig. 3 the effect of the hop attack on authentication times

In this simulation, the malicious nodes change the hop number of messages to 0. As shown in Fig.3, authentication times increase with the attack intensity increasing, but in the hop attack it is more than in the no-hop attack. Even if malicious nodes change the hop number, the throughput of DWMA still achieves at least 87%, and the possibility that malicious nodes are detected successfully reaches at least 90%. So the hop attack increases the authentication times and the energy consumption in some degree, but that doesn't affect the security work of DWMA seriously.

4. CONCLUSION

There are many types of DOS attacks, and it is very difficult to resist DOS attacks. To be able to make use of digital signature to verify data and limit DOS attacks, this paper proposes DWMA. DWMA allows that sensor nodes could decide whether to authenticate data by itself, thus could save much energy. The simulation results show that DWMA is effective and flexible, and the energy consumption of DWMA using digital signature is as nearly the same as that of the per-hop authentication using MAC

In order to evaluate DWMA completely, we need to further study the distribution of W of sensor nodes for neighbor nodes. Meanwhile, the functions and the parameters about the window value and the window growth delay degree are very significant in DWMA. In the future, we will consider how to set the functions and the parameters according to different application environments of WSN.

5. ACKNOWLEDGEMENTS

This work is supported in part by the National Basic Research Program of China (973 Program) under grant No. 2006CB303000 and is funded by the Fundamental Research Funds for the Central Universities (22005010).

6. REFERENCES

[1] Raymond D.R, Midkiff S.F."Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses". IEEE Pervasive Computing, vol.7, no.1, pp. 74-81, Jan.-March 2008.

[2] Adrian Perrig, Robert Szewczyk,J. D. Tygar,Victor Wen,David E. Culler ."SPINS: Security Protocols for Sensor Networks". Wireless Networks, vol.8, no.5, pp.521-534, Sep 2002.

[3] Luk M, Mezzour G Perrig A, Gligor V. "MiniSec: A Secure Sensor Network Communication Architecture". IPSN 2007, pp. 479-488, 25-27 April 2007.

[4] Sencun Zhu, Sanjeev Setia, Sushil Jajodia, Peng Ning. "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks". ACM Transactions on Sensor Networks, vol. 3, no. 3, pp.14/1-14/33, August 2007.

[5] Kui Ren, Wenjing Lou, Yanchao Zhang. "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks". IEEE Transaction on mobile computing, vol. 7, no. 5, pp.585-598, May 2008.

[6] Jing Deng, Richard Han, Shivakant Mishra. "Limiting DoS attacks during multihop data delivery in wireless sensor networks". International Journal of Security and Networks, vol.1, nos.3/4, pp.167-176, 2006.

[7] Wander A.S, Gura N, Eberle H, Gupta V, Shantz S.C. "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks". PerCom 2005.Third IEEE International Conference, pp. 324 – 328, 8-12 March 2005.

[8] David J. Malan, Matt Welsh, Michael D. Smith. "Implementing public-key infrastructure for sensor networks". ACM Transactions on Sensor Networks, vol.4, no.4, pp.1-23, Aug.2008.

[9] Ronghua Wang, Wenliang Du, Peng Ning ."Containing denial-of-service attacks in broadcast authentication in sensor networks". 8th ACM MobiCom, pp.71-79, Sep 2007.