Enhancing Base Station Security against DoS Attacks in Wireless Sensor Networks

Zhen Cao, Xia Zhou, Maoxing Xu, Zhong Chen, Jianbin Hu, Liyong Tang
Information Security Laboratory
School of Electronics Engineering and Computer Science
Peking University, Beijing, P. R. China
{caozhen, zhouxia, xumx, chen, hjbin, tly}@infosec.pku.edu.cn

Abstract—In this paper we propose a reputation based client puzzle scheme included in a security framework to enhance base station security against Denial-of-Service attacks in the scenario of wireless sensor network. Through flexibly adjusting the difficulty level of puzzle according to each node’s reputation value, we make malicious nodes with low reputation value face harder puzzle, rendering their attacks tougher while limiting extra overhead to normal nodes. We analyze our security framework in the specific case of SPINS, and conduct simulation to evaluate its effectiveness.

Keywords—DoS; Client Puzzle; Reputation

I. INTRODUCTION

Recent years have witnessed the rapid development of wireless sensor networks, whose notable structure is hierarchy, rooted in a base station connecting multitudes of resource-constraint sensor nodes collaborating together to accomplish specific task ranging from civilian to military applications.

On one hand, these distributed systems of smart sensors have potential to revolutionize the way in which the real world is monitored and controlled. On the other hand, such network also imposes a series of security challenges to network designers especially in the scenario of military applications which has attracted research interests all over the world [1][2]. Among those security problems, Denial of Service attack defined as any event that diminishes or eliminates a network’s capacity to perform its expected function [2], degrades network’s intended service to its users, thus is considered one of the most general and dangerous attacks endangering network security. We will address this very problem in this paper.

As for DoS vulnerabilities, different part of the network undergoes quite a different story. Essentially we can partition the overall network into three parts, and we argue that countering DoS attack actually should be considered distinctively within those parts. The first part is the ad hoc network of all those sensor nodes working together for data collection or monitoring. Because a few broken nodes will not apparently impact the performance of the whole network, DoS attack within this part brings trivial benefits to attacker. Secondly as for the connection part between base station and outside network as well as ultimate user, each terminal in this context usually owns strong power and capability resulting in the difficulty for attackers to launch DoS attack towards them.

Therefore, DoS attack in this part also is not severe. Lastly, let us turn our attention to the connection part between base station and the ad hoc sensor network. Base station not only acts a key part that aggregates data reported by sensors and disseminates queries requested by users, but also offers security service to routing protocols such as SPINS [3] and INSENS [4]. Therefore it is worthy a great deal for attackers to break it down thus failing the whole network. In this regard, enhancing base station security against DoS attacks is generally considered as a most urgent and significant issue.

With this bear in mind, we propose a security solution framework tailored to the base station for its defending against DoS attack. After initial DoS detection and analysis prerequisite, base station challenges clients with cryptography puzzles to protect itself. Compared with traditional puzzle schemes, we introduce the novel reputation based client puzzles, which applies a dynamic policy to adjust the puzzle difficulty for each node in terms of node’s reputation value, so that the punishment for malicious nodes becomes more and more pressing without introducing extra unnecessary burden to most normal nodes. Moreover, we systematically present definite details of our solution framework through the case study of SPINS [3] protocol.

This paper is organized as follows: in section 2 we summarize some relative works on DoS attack countermeasures and the ways to secure base station against various threats. Then our framework for enhancing base station security against DoS attack is elaborated in section 3, which is followed by a specific case analysis in section 4. At last we conclude the paper in section 5.

II. RELATED WORK

There are numerous research works [2, 5-9] devoting to the strategies of avoiding or countering DoS attack. Among them client puzzle method offers many advantages over others. In fact, its idea can be traced back to [6], which required client to solve a puzzle generated by the server before sending data to it. Typically a puzzle is composed of moderately-hard function, and can only be solved through brute-force searching within solution space. In this way server imposes computational burden on the clients making it harder for malicious node to launch DoS attack towards server. Besides computation based puzzles, recently other forms of puzzles are also actively studied, such as memory bound puzzle proposed by Abadi et
al.[7], utilization of reverse Turing tests as puzzles in [8] and so forth.

Though all these discussions on the countermeasures of DoS attacks are not tailored to wireless sensor networks, they do convey lots of valuable and heuristic hints to our consideration under the context of wireless sensor networks. In fact, the topic of how to counter DoS attack in wireless sensor networks is not a nascent one for the considerable works [10-13] dedicated to it. Specially [2] detailedly analyzed DoS attack existing in wireless sensor network from the perspectives of all the network levels, and pointed out it is desirable to take this concern into account at the phase of initial network design.

In wireless sensor network, the security of base station plays the key role since its failure breaks down the whole network. Deng et al. [10] proposed to use multi-path routing to tolerate intrusion in sensor network. Then in [11] they further proposed two other methods besides multi-path to secure base station against malicious attacks, which are the disguising of base station location and the relocation of base station.

Our work differentiates from the aforementioned works in that we propose an integrated security framework for the preliminary network design, incorporating a flexible reputation based client puzzle scheme to protect base station against DoS attack. To the best of our knowledge, this is the first work to adopt client puzzle aided by a reputation scheme in wireless sensor network for base station security.

III. SYSTEM MODEL

In this section, we present our threat model and system framework as a basis of the further case study in section 4. Note that we just propose the overall security framework for base station here, instead of involving each module’s specific details, which will be showed explicitly through the systematic case analysis in latter section.

A. Threat Model

Three kinds of entities exist in our network: the base station, attackers and common sensors. Utilizing the flaws in the communication protocol, attackers threat the base station through flooding. Namely attackers send many connection establishment requests to the victim, making it engaged in dealing with those meaningless packets while preventing legitimate nodes from connection.

In our model there is no drastic discrepancy between the capacity of attacker and normal node. Since the whole procedure of solving puzzle brings down attack frequency, solving the puzzle still composes a threat to attackers who will definitely try to elude this. Besides, we assume that global information of the network is unavailable to attackers, and base station is capable to obtain the traffic information provided by the secure routing protocol such as SPINS [3] and INSENS [4].

B. Solution Framework

As what the Fig. 2 indicates, our integral security framework for base station includes three modules, which are detection module, response module and protection module respectively. They are designed to be deployed at base station for security enhancement.

The responsibility of detecting module is twofold. Firstly through monitoring the traffic towards base station it records them in the form of routing sets, which consist of the pair \(<\text{Path ID}, \text{Source node ID}>\) mirroring each path. Then it performs further analysis based on above records and delivers statistical result to response module, which exploits a threshold mechanism to decide whether to trigger the next module.

The most characteristic part in our framework is protection module, which is built upon client puzzle scheme combined with a dynamic adjustment scheme based on reputation value. When the base station detects that it is under severe attacking, it challenges all nodes including potential attackers with client puzzle. As all nodes are then forced to consume more energy and computation resources to solve the puzzle questions for subsequent communication, attacks turn out to be expensive and ineffective for attackers. Meanwhile considering the increased cost for other normal nodes to keep communication with base station, we propose a flexible scheme to give puzzles of different difficulty level to different nodes according to their respective reputation values. In this way, our “reputation based client puzzles” (RBCP) scheme diminishes the side effects brought by traditional client puzzle mechanism to honest nodes.

![Figure 1. A Framework Defending DoS attacks](image-url)

The core idea of reputation based client puzzle (RBCP) scheme is that, the higher reputation value the node owns, the easier puzzle question should be given to this. Besides, we assume that global information of the network is unavailable to attackers, and base station is capable to obtain the traffic information provided by the secure routing protocol such as SPINS [3] and INSENS [4].
myriad packets resulting in a great \( n_g \), and reluctant to solve
the client puzzles leading to small \( n_p \). Hence the difficulty of
puzzles for attackers will increase according to low reputation
value, whereas for honest nodes, who honestly solve
puzzles give rise to larger \( n_p \), will get high reputations
mapping to easier puzzles. In this way, reputation value helps
tell honest nodes from malicious ones so that they can be
treated distinctively.

IV. CASE STUDY

In this section we apply our solution framework proposed
in Section 3 to defend base station against Denial-of-Service
attacks in a specific scenario. Taking the key agreement
protocol proposed in SPINS [3] for an instance, we introduce
specific detail of each module in order to exhibit how the
aforementioned framework works in practice.

A. SPINS Key Agreement Protocol

Fig. 2 shows the message exchange process of the key
agreement protocol in SPINS. Here \( A \) and \( B \) represent
two participants who want to set up a secret key \( SK_{AB} \) with the help
of base station \( S \). \( N_A \) and \( N_B \) are the nonce generated by \( A \) and
\( B \) respectively. \( S \) shares secret keys \( KS_A \) and \( KS_B \) with \( A \) and \( B \) respectively.
MAC is a message authentication code algorithm.

\[
\begin{align*}
\text{Step 1.} & \quad A \rightarrow B: N_A , A, \\
\text{Step 2.} & \quad B \rightarrow S: N_B , A , B , MAC(KS_B , N_A | N_B | A | B), \\
\text{Step 3.} & \quad S \rightarrow A: \{SK_{AB} | KS_A , MAC(KS_A , N_A | A | \{SK_{AB} | KS_B \}), \\
\text{Step 4.} & \quad S \rightarrow B: \{SK_{AB} | KS_B , MAC(KS_B , NB | A | \{SK_{AB} | KS_B \}).
\end{align*}
\]

Figure 2. Key agreement protocol in SPINS

In this protocol base station is susceptible to a potential
denial-of-service attack, where \( A \) keeps sending \( Msg1 \) to many
other nodes so that base station \( S \) will soon be overwhelmed
with myriad \( Msg1 \) from \( A \) just now. Without any identity
verification, \( S \) has to consume much more computation
resource to check the integrity of the message and then
construct two messages sent back to \( A \) and \( B \) for key
distribution. What’s more, base station need to store the status
information including \( N_A \), \( N_B \), \( KS_A \), \( KS_B \) and \( SK_{AB} \)
causing attackers’ simple flooding of \( Msg1 \).

B. Detection and Response

Through periodically analyzing statistical routing
information, base station adopts suitable response policy
in terms of current network situation, which can be exhibited by
the percentage \( e \) of attackers in the network. In order to
estimate current fraction of attackers, base station firstly
calculate the formulation below to get a \( gap_k \) value, which
indicating the capacity discrepancy between the nodes of two
parts split by node \( k \).

\[
gap_k = \frac{\text{avg}(n_i | n_i > n_s)}{\text{avg}(n_i | n_i \leq n_s)}
\]

Here, \( n_i \) denotes the times for node \( i \) appearing as a source
node in each pair of the routing set.

Let us use \( gap_{max} \) of node \( n_{max} \) denoting the maximal value
of \( gap_k \), namely \( gap_{max} = \max (gap_k) \). Since generally there is
significant difference between attackers and common nodes on
the appearance frequency as source node in each pair of
routing set, we can take those nodes \( i \), whose \( n_i \) are larger than
\( n_{max} \), for attackers. Then we can get the percentage of attackers
by calculating the expression

\[
r_m = n_m / N_m,
\]

where \( n_m \) is the number of deemed attackers while \( N_m \) denotes the total number of
nodes.

Once \( r_m \) exceeds a threshold, response module will trigger
the initiation of protection module to hold back attackers. Note
that the threshold value, as a parameter representing the
network’s sensitivity to DoS attack, can be predefined by
network administrator.

C. Reputation based Client Puzzle

Apart from the requirement that attackers cannot solve the
puzzle in advance or replay puzzle solution from other nodes,
the construction of puzzle should also meet such principle that
compared with its verification its solving is far more arduous
[14]. Moreover initiator and responder need to generate
session identifiers \( SII \) and \( SIR \) for each different session
respectively rendering the pair \( (SII, SIR) \) unique.

\[
\begin{align*}
\text{Step 1.} & \quad \text{Set up the session identifiers. } SII = N_A, \ SIR = \\
& \quad \text{HMAC(secret, SII/ID_{i}), where secret is the local key changing with time and only known to the base station. } \ SII \ \text{and } \ SIR \ \text{are both 64-bit long.}
\end{align*}
\]

\[
\begin{align*}
\text{Step 2.} & \quad \text{Construct puzzles. The puzzle is defined as finding a } 16\text{-bit solution to guarantee all the left } k\text{-bit of }
& \quad \text{Hash(SII/SIR/solution) is zero. Note that here the value of } k
\end{align*}
\]

\[
\begin{align*}
\text{Step 3.} & \quad \text{Adjust puzzle difficulty. The adjustment of puzzle difficulty is based on the reputation value computed through formula (*). Given current detected fraction of attacker } r_m,
& \quad \text{base station raise the difficulty level of puzzles for those clients with } r_m \text{ lowest reputation values through increasing the value of } k,
& \quad \text{and meantime lower the difficulty of puzzles for others. This step must be finished within a reasonable time slot}
Given that hash function, the initiator
has no way to figure out solution other than brute force
searching the solution space. This searching process will force
the clients to compute hash function for } 2^k \text{ times even in ideal case. The value of } k
\end{align*}
\]

\[
\begin{align*}
\text{D. Evaluation}
\end{align*}
\]

Deluge [15] gave detailed performance for cryptography
primitives in TinyOS environment. Take SHA-1 algorithm for
an instance, its computing averagely takes 14ms. As a result,
we can estimate the average time for solving a puzzle in terms of the specific time for computing adopted hash function.

We simulated the scenario consisting of 100 nodes, which send packet to base station at random interval. Considering attacker’s motivation, we set the overall packet sending frequency of malicious node apparently higher than that of normal nodes. And puzzle computation is simulated by decreasing their packet sending frequency. Base station owns buffer to store packets from sensor nodes and processes them one by one with equal processing time. Moreover, it denies any more packets from normal nodes once buffer is full. In this sense, the duration when buffer in base station is full properly depicts the DoS attacking level. Hence we utilize it as a criterion to evaluate the effects of client puzzle scheme.

In Fig. 4 we show the effect of reputation based adjusting scheme on the loss rate of normal nodes’ packets. Upper line indicates the case when introducing reputation based adjusting scheme. As it is always below the line which mirrors the case without adjusting scheme, we can conclude that reputation based adjusting scheme reduce the negative influence on normal nodes thus further optimizing client puzzle scheme.

V. CONCLUSION

Base station which affords secure service to end users plays so crucial a role in wireless sensor networks that its security against denial-of-service attack is vital and urgent. Our security framework for base station is proposed to defend it against DoS attacks via a novel reputation based client puzzle method, and its effectiveness is proved through simulation results.

REFERENCES