Research on key management scheme for military internet of things

Haopeng Li[1,a] ,Liyun Chen[1,b],Jie Yan [2] ,Wenxin Qiao[1]

[1]Department of Information Engineering,Ordnance Engineering College,Shijiazhuang,050003,China
[2]Luoyang Electronic Equipment Testing Center,Luoyang,471000,China
[a]lhpkkkk@126.com,[b]493376952@qq.com,

Abstract: Aiming at the problem of insufficient security protection in military internet of things under mobile state, a scheme of node key management on navigation system is proposed. By comparing the node-related data with the set strategy, it can complete the node's Key distribution, renewal and destruction. The analysis shows that the scheme has high security and survivability, and has played an important role in protecting the security of military internet of things.

Keywords： military internet of things,key management,security

1. Introduction

The development of military things has just started,the technical conditions are not mature enough and it is facing with a variety of challenges[1]. In particular, the problem in the Internet of Things is more prominent than that of the traditional communication network. Due to the lack of node protection and the shortage of resources, the security of the node is frequent. The communication of the node is easy to be stolen or intercepted[2]. The probability of leakage is greatly improved, so its safety issues should be widely concerned. Therefore, it is necessary to provide the necessary protection measures for the Internet of Things in terms of mechanism and technology so that it can be safety, stable and efficient[3]. As the key technology of Internet of Things security, key management can effectively protect the perceived node information and the whole thing network system security[4]. The literature[5] proposes a grid-based key mechanism to establish key pairs only between adjacent nodes to eliminate the adverse effects of other nodes. The literature[6] proposes a wireless sensor network key management protocol based on elliptic curve cryptosystem, which has strong extensibility and anti-attack. The literature[7] proposed a time-based random key management scheme, which uses a two-level random key pre-allocation mechanism to improve the utilization of node resources and strengthen The node's resistance to damage. The literature [8] proposed a deployment of information based on the wireless sensor key management program, the program has better performance. In my paper, based on the Beidou navigation system, the node node dynamic information is provided to determine the state of the node, and the distribution, update and destruction of the control node key are achieved. The key management technology based on Beidou navigation system can better adapt to the security needs of complex battlefield environment, and more effectively resist the enemy's cyber attack.

2. Key Management scheme for Military Internet of Things

2.1 Key Distribution

That the key can be safely distributed to each node is the first gate that guarantees the key security, which is the primary condition to guarantee the security of the whole military internet of things system.

When the key is distributed, the node first accesses the Beidou satellite navigation system through the active terminal equipment and performs the registration. The system uses the short message security channel provided by Beidou RDSS in an active or passive way according to the request of the node and the key management strategy set in advance to realize the unicast key distribution to the Beidou network user. Generally speaking, general network will set the key management center. In view of the characteristics of low-power, low-rate of the Internet of things, in order to reduce the communication costs of the network, Internet of things uses the distributed lightweight CA key management framework, revokes the key management center. After generating the node key pair, the cluster nodes are distributed through the cluster head. The inter-cluster nodes are uploaded and distributed to the cluster head nodes of other clusters through the security channel of Beidou short message. The cluster head node is then issued in turn, In the entire process of key distribution, internet of things are used in unicast way. The key is distributed through the Beidou safety channel as shown in Figure 1.

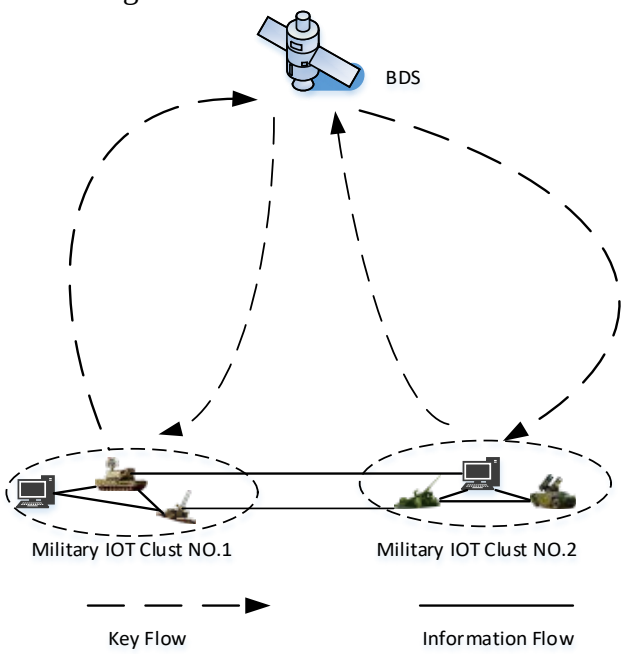

Figure 1. Schematic diagram of key distribution of military Internet of Things

2.2 Key update

Key update is an important part of key management, to ensure that each node's key in the system of the military internet of things always maintain freshness, which can effectively prevent the node to be broken through by the enemy.

For the Beidou network users (nodes of military internet of things) which have been registered and connected to the Beidou satellite navigation system through the active terminal equipment, the precise time, position and speed information provided by the Beidou satellite navigation system are used. According to the pre-set key management strategy, through the trusted channel of Beidou satellite navigation system, the management of key update of the key of Beidou network users is realized,

and the complexity of key management is reduced, while the space-time segmentation and precise management of the key of Beidou network users are effectively realized. The key update in military things of internet consists of the following three phases: key initialization, node status query, key update. Where the initialization of the node's key is done only once, that the state query and key update are carried out in a pipelined structure, and the two phases can overlap in time, and the query time is generally longer than the update time. The phase that node states query is operated through the Beidou navigation system, to ensure that the node can update the key in the case of synchronous clock. The process of key updating based on the Beidou navigation system for states querying as shown in Figure 2.

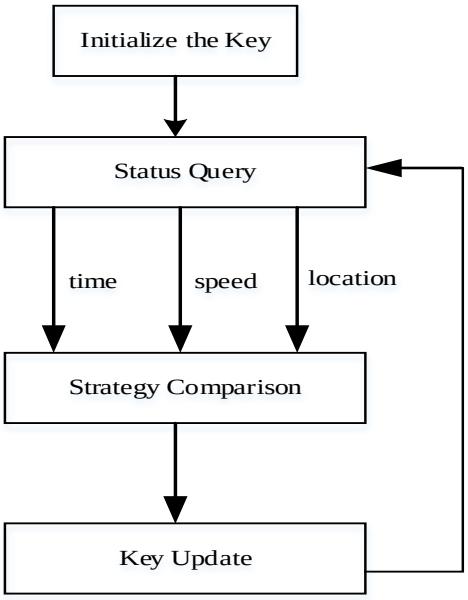

Figure 2. The process of key updating of military Internet of Things

2.2.1 Key initialization

All nodes in the military things of internet are positioned through the Beidou navigation system, are divided into different areas. After networking, each node in the area exists as a separate network. A number of nodes are selected as a lightweight CA based on the public key authentication framework of lightweight CA, use distributed authentication method to generate the public and private key pairs of each node, thus completing the initialization of the key. Whenever there is a new node to join, identify the location through the Beidou navigation system. After the node is identified as the nodes of military internet of things, generate key pairs through the lightweight CA.

2.2.2 Status query

Through the time T, Beidou navigation system for all nodes in military internet of things queries the status information, informs node's real-time location information, synchronizes clock information, speed information.

2.2.3 Key update

Compare the collected the relevant state information through the timing, positioning, speed measurement function of Beidou navigation system with the key update strategy. For a node that triggers a rule, a new key pair must be generated by the lightweight CA to replace the original key to ensure the security of communication between nodes.

2.2.4 Update policy settings

The Beidou navigation system obtains the node time, location and speed

information through conducting timing, positioning and speed measurement on nodes in the military internet of things which have been equipped with Beidou module, and the setting of the node key's update policy is as follows:

1) Set the normal cycle time T, the node key is updated once every time of a cycle (the value of T is appropriate).

2) By checking the node freshness in the network, when exceeding the maximum response time t of the set node, the node key is updated once and the node freshness in the network is re-examined (t is far less than T).

3) The node key is updated once when the different subregions are delimited globally and the node position is changed from one combat zone Z_1 to another combat area Z_2.

4) Beidou navigation system positions nodes within a short time the movement trend of which deviate from the predetermined direction, the node's key updates once.

5) The node moves faster than the preset maximum speed V_1, and the node updates the key once.

2.3 Key Destruction

In the key management, it is necessary to consider the security of the key generation and distribution stages while ensuring that the revocation of the key is safe and effective. When the node security in the military internet of things has a problem (the node is captured, etc.), it is necessary to ensure that the node's key destruction mechanism plays a role, and the timely destruction of the node's insecure key ensures that the entire military internet of things is in a safe state in subsequent communications.

2.3.1 The basic process of destroying

Key destruction is complementary with the key update. In the phase of status query, if the node is in an abnormal state, the control center will issue the identity confirmation information to the node. If the response is not received within the specified time or the response is wrong, it is judged that the node has been invalidated. At this point, the key destruction rule is triggered and the key of the failed node in military internet of things will be destroyed. The KeyRev scheme is used to prevent the failed node from generating a new session key and destroy all the key replicas at the same time, so that the failed node can't participate in any communication in the Internet of things.

2.3.2 Destroy policy settings

Key destruction strategy is also divided into three categories, the specific strategy set as follows:

1) Communication between nodes, the response node needs to exceed the maximum response time n times, then determine the node has failed, and destroy the node's key and its copy.

2) By locating the node, the node is not scheduled to move in the designated area according to the scheduled plan and is not authorized to enter the other area. Then it is determined as the failure node and the key and the copy of the node are destroyed.

3) If the node exceeds the guaranteed safety speed V_2 or fails to follow the instruction, the key of the node and its replicas are destroyed.

Through the pre-set update and destruction strategy, compare the collected information with the rules, you can complete key destruction management in the military internet of things , the diagram of overall structure as shown in Figure 3.

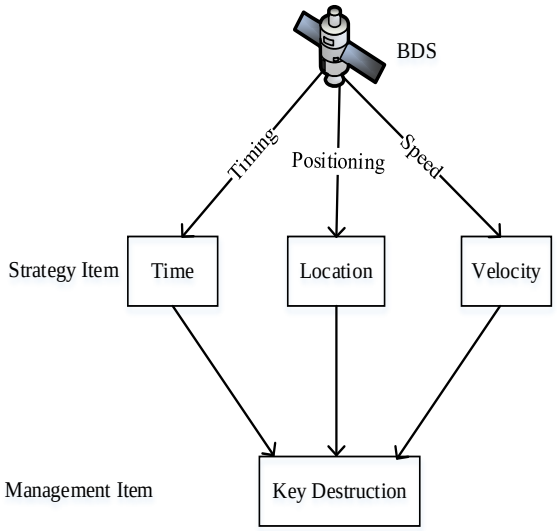

Figure 3. Schematic diagram of key destruction based on the default strategy

3. Performance analysis

3.1 Efficiency analysis

Nodes in military internet of things can use the highest level of the Beidou card, the maximum transmission volume is 240 characters each time, the maximum sending frequency can up to once per minute. In the stage of key distribution, the communication traffic of the distribution of keys through the Beidou channel is less than that through the Beidou short message channel, so to meet the minimum standards of key management, calculate the average transmission delay through the Beidou short message channel, we can find the average transmission delay is proportional to T_i.Set m is the total number of packets to be transmitted and received, T_{i1} is the i-th packet transmission time, and T_{i2} is the i-th packet acceptance time.Taking a sample set of data for m = 3500 times the simulation experiment can get an average transmission delay of about 2.66s. In the case of emergency or network requiring high security, you can think that the efficiency is relatively high. In the phase of key update or key destruction, the collected information data for the time, location, speed and other short string are generally defined 15 to 30 characters. After be encrypted by a one-way hash function, the data can also be multiple to send, and military internet of things use the military band of Beidou navigation system that is different from the civilian dedicated channel, Beidou navigation system will be judged as high priority events for processing when take the operation of key management, In summary, this mechanism can maintain a high efficiency.

3.2 Extensibility analysis

The addition or exit of a node in the military internet of things does not affect the key management of the other nodes. It only needs to distribute or revoke the key in real time to complete the update of the node. Therefore, the mechanism has good scalability.

3.3 Security analysis

An eavesdropping attack refers that non-network members steal data of communication between groups of nodes. If the eavesdropper is a non-network member, he can not obtain the relevant key information such as the key of update packet encryption key in the network or prompt message. Therefore, he can only attempt to obtain the data packet by exhaustive search attack and analyzes it, such an

attack overhead is O（2^n）, where n is the length of key, so that the overhead can be seen as infinity, it can be to some extent to prevent eavesdropping attacks.

Active attack refers that the current team members steal the data of communication between groups of other nodes. Through group nodes can be synchronized time through the Beidou navigation system, to understand the strategy information of the group within a certain time, but can not obtain the location information and speed information of other nodes. Three kinds of information can not be obtained at the same time, you can not pass the identity authentication between nodes, that is, unable to crack encrypted communication packets. If the node leaves the group and wants to retrieve the key of new group node by looking up the table attack, it must compute a data table based on the previous key. The workload of the method is no less than the amount of exhaustive search attack, so this mechanism can effectively prevent active attacks.

4. Concluding remarks

Facing to all kinds of security problems for military networking, the paper proposes a key management scheme for military internet of things.The nodes' state information can be collecting by Beidou navigation system timing, positioning and velocity measuring.Comparing with setted steategies,it can achieve the keys' distribution,updation and destruction,it can keep the military internet of things safety. The performance analysis shows that the key management scheme can maintain high efficiency and good security.

References

[1] Zeng Ping, Zhang Li,Yang Yatao, et al.A key management scheme for internet of things based on HECRT[J].Computer Engineering,2014,40(8):27-32,37.

[2] Li Wei, Gu Dawu, Zhao Chen, et al.Security analysis of the led lightweight cipher in the internet of things[J].Chinese Journal of Computers,2012,35(3):434-445.

[3] Yu Xiaoan, Xia Bing, Cao Shaojun. Key management of ammunition network based on location and time combination[J].Journal of Detection & Control,2014,36(6):45-49.

[4] Pan Zhibo, Zheng Baoyu, Wu Meng. Study on a key update mechanism for secure multicast based on time stream[J].Journal of Electronics & Information Technology,2004,26(7):1045-1052.

[5] Li Ming, Xiong yan, Miao Fuyou. Grid-Based Predistribution Secret Key Mechanism for Wireless Sensor Network[J].Computer Engineering,2011,37(19):107-110.

[6] Jian Bo, Cuo Yanghui, Luo Changyuan, et al. Key management protocol for WSN based on ECC[J].Computer Engineering,2010,36(3):142-144.

[7] Yuan Ting, Ma Jianqing, Zhong Yiping, et al.Key management scheme using time-based deployed for wireless sensor networks[J].2010,21(3):516-527.

[8] Zhang Juwei, Sun Yugeng. Pairwise key pre-distribution scheme for wireless sensor networks based on deployment knowledge[J]Computer Engineering and Applications,2008,44(20):4-6.