An Energy-efficient Secure AODV Protocol in Industrial Sensor Network

Weidong Fang[1,2], Chuanlei Zhang[3], Wei Chen[4], Ming Li[4], Fengying Ma[5]

[1] Key Laboratory of Sensor Network & Communication, Shanghai Institute of Micro-system and Information Technology, Chinese Academy of Sciences, China
[2] Shanghai Research Center for Wireless Communications, China
[3] School of Computer Science and Information Engineering, Tianjin University of Science and Technology, China
[4] School of Computer Science and Technology, China University of Mining and Technology, China
[5] School of Electrical Engineering and Automation, Qilu University of Technology, China
wd_fang@126.com, a17647@gmail.com, {chenw, lmgyw}@cumt.edu.cn, mafengy@163.com

Abstract

As a traditional routing protocol, the Ad hoc On-demand Distance Vector routing (AODV) protocol has been applied in many industrial sensor network (ISN) fields. Meanwhile, researches on AODV mainly focus on improving performance and enhancing security. Unfortunately, there are a few researches on joint energy efficiency and security. In this article, we proposed an Energy-efficient Secure AODV Protocol (E-SAODV) for industrial sensor network. In E-SAODV, the Low Complexity Verification Mechanism (LCVM) is introduced, and the Delayed Transmitting Mechanism (DTM) is proposed and applied. In LCVM, the polynomial of CRC-4 is introduced to substitutes RSA digital signature in SAODV, in order to guarantee the integrity of data verification, and reduce storage space, computation and energy consumption. The DTM is implemented to separate the checksum and valid data, achieve the tamper-proof. The simulation results demonstrate that comprehensive performance of E-SAODV is a trade-off between energy efficiency and security, and with better performance than AODV and SAODV.

Keywords: Industrial sensor network, Security, AODV, Energy efficiency

1 Introduction

As the emergence and development of the Wireless Sensor Network (WSN) [1], the Cloud Computing [2], the Big Data [3] and the intelligent terminal, the Industrial Sensor Network (ISN) [4] has become an important application of the sensor network in industrial field. The Industrial Sensor Network is an interdisciplinary research hot spot, which involves the automation, the computer, the communications and the management sciences. From the view of current technology development and application, the requirements of ISN mainly focus on the following fields: Supply Chain Management [5], Localization [6], Optimization of Production Process [7], Equipment Monitoring and Maintenance [8], Vehicular Network [9] and so on.

Generally, the mobile/fixed nodes achieve to collect information in dangerous and unreachable areas, on the other hand, the short-range wireless communication implements to converge and transmit information in ISN. Unfortunately, the particularity of the industrial environment makes applications of ISN have to consider some adverse factors: the wireless signal multipath caused by reflection and scattering of large-scale equipment and metal pipes, the interference to wireless communications caused by electromagnetic noise, which generated by the motor and equipment operation. Especially, in industrial production process, the key point of ISN's application is secure transmission of production process parameters. This is due to that network information security is facing a growing challenge. The possibility that controls systems of industrial facilities is damaged by network intrusion. Perhaps, this loss of risk may be too large to measure.

The promotion of open network technologies improve industrial data rate of transmission, and reduce the integration of information technology on the one hand. It also makes network security become more challenging. The information security in Industrial Sensor Network mainly involves information sensing security and network transmission security. Meanwhile, the low-power technology has been one of the hot topics in ISN [10]. In this paper, an energy-efficient secure AODV (Ad hoc on-demand distance vector routing) protocol (E-SAODV) is proposed to meet the requirements of defense against the attack and low-power in Industrial Sensor Network. The rest of this

*Corresponding Author: Wei Chen; E-mail: chenw@cumt.edu.cn
DOI: 10.3966/160792642018011901023

paper is organized as follows: Section 2 gives a brief review of AODV and its evolution. Some preliminary knowledge and secure requirements are represented and analyzed in Section 3. The E-SAODV protocol is proposed, and simulation results and analyses of the proposed protocol are presented in Section 4. Finally, some concluding remarks are provided in Section 5.

2 Related Works

As a traditional routing protocol, AODV protocol has always been a research hot spot. At presented, the research on AODV is classified as two categories: one is focus on enhancing its security to defend against many attacks; the other is improving its performances, such as reliability, and transmission performance under dynamic topology.

2.1 Security Enhancement

Under most circumstances, the design of AODV protocol does not take account for security. However, with the increase of security issues, various secure schemes have been researched and proposed to meet different application requirements. These schemes mainly detect and defense against some specific attacks. In recent years, the researchers on AODV's security have focused primarily on sinkhole attack, blackhole attack and Sybil attack.

Gandhewar and Patel proposed a scheme for detection and prevention of Sinkhole Attack on the context of AODV protocol [11]. This scheme of detection & prevention considered the behavior of sinkhole attack and AODV working, which mainly consist of four phases: the initialization phase, the storage phase, the investigation phase and the resumption phase. The scheme could improve the performance of AODV under sinkhole attack. Singh and Chaurasia put forward the scheme of detection and isolation of sinkhole attack in MANET [12]. The key point of this scheme is that a threshold value of sequence number was assumed based on average sequence number of packet to successfully received/transmitted by the destination and source node. If the value of sequence number in received packets is larger than then it is widely accepted that packet may be malicious. Xiong et al. adopted the FP-Growth (Frequent Pattern Garwth) according to the AODV route table information, gave s rank sequence method for detecting black hole attack in ad hoc network [13]. This method could exclude many normal nodes before the DE-Cusum (Data Efficient Cusum) detection because the normal node had a stable rank in a sequence. Particularly, when the wireless environment became stochastic, the detection of rank sequence was better than the detection of distribution. Gupta proposed a new method RTMAODV (Real Time Monitoring AODV) [14], which used the concept of broadcasting. In this method, node that replied to Route Request (RREQ) by source was being monitored in any mode. Detection of malicious node was actually done by neighbor node of Route Reply (RREP) transmitter node. The method did not introduce any overhead. The neighbor node detected and prevented black hole attack using real time monitoring. Syed et al. proposed a solution to avoid Black hole attack in AODV [15]. This solution used a route legitimacy value attached with RREP which ensured that the route was free from black hole node.

As above mention, almost all of secure schemes and secure protocols in AODV only detected and defended/mitigated against the special attack. However, these secure techniques seemed seldom to consider the energy efficiency.

2.2 Performance Improvement

AODV is a distance vector routing protocol [16]. It supports intermediate nodes to reply, makes source node quickly obtain routing, and effectively reduces the number of broadcast. Since the nodes only store on-demand routing, the scheme reduces the memory requirements and unnecessary duplication. However, because of periodically broadcast packets, a certain energy consumption and network bandwidth have to be considered. Due to the existing of stale routing, AODV requires a relatively long latency to establish routes. Currently, the performance improvements of AODV mainly involve in the following areas: energy efficiency, improving throughput, load balancing and especially, in industrial field.

Jain and Suryavanshi proposed a new maximum (MAX) energy Local Route Repair (LRR) approach with multicast AODV routing protocol [17]. These schemes included two processes: the establishing path and the forwarding packets from source node to destination node. The transmitter always selected the next neighbor node which had maximum energy in network. Due to the energy depletion and mobility of node, the LRR scheme reestablished the path from the same end. The proposed LRR with multicast AODV could improve the network performance and reduce the energy consumption in network. Joshi and Kaur aimed at improving the Infrastructure based AODV (I-AODV) routing by considering V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) communication. I-AODV routing protocol facilitated communication among vehicles through RSUs (Road-Side Units) and broadcasted in nature. They discussed the prediction based on multicasting which aided in reducing delay and improves other performance metrics, and applied multicasting to solve the purpose of proper utilization of resources, as well as prediction technique helped in improving localization overhead [18].

For congestion issue, Bansal et al. proposed a system and modified the existing AODV algorithm by using congestion control phenomena [19]. In proposed

system, the node waited for acknowledgement for the threshold period of time. If the acknowledgement was not received with in threshold period, then the node broadcasted again to select alternate path. Ranjan et al. proposed Improved Optimum Angle Selection AODV (IOAS-AODV) routing algorithm [20], which avoided the congestion and repair the broken link by choosing a set of limited nodes for alternate route based on the quadrant position, battery status, queue length, and forwarding region. The IOAS-AODV could improve the routing performance such as the throughput, the end to end latency, the routing overhead, and the packet delivery ratio.

From the above analysis, the enhancing security and the improving performance have been research in AODV. Unfortunately, the joint works of above two aspects are seldom researched. Therefore, we will propose an Energy-Efficient Secure AODV Protocol (E-SAODV) in the following sections.

3 Preliminary Knowledge & Analysis

3.1 AODV

AODV (Ad hoc on-demand distance vector routing) is a source driven routing protocol [16], it could realize dynamic, bootable and multiple hops routing between mobile nodes, which are useful to establish and maintain the Ad hoc network. Because of the similarity between the Ad Hoc network and the sensor network, the AODV protocol could also be used in the sensor network. AODV protocol allows the mobile nodes to get the routing quickly and respond to link disruption and the network topology changes regularly. AODV protocol is non-cyclic, which avoid the Bellman-Ford "infinite computing" problem and could converge rapidly when the network topology changes. AODV will notify the affected nodes to avoid using the broken links when the link is destroyed.

The two phases of AODV protocol is described as follows:

Route discovery. In this phase, the *RREQ* (Route Request) packet is transmitted by the source node. *RREQ* packet contains the source identifier (*SId*), destination identifier (*DId*), serial number (*SSeq*), destination sequence number (*DSeq*), broadcast identifier (*BId*) and *TTL* (Time To Live). When a *RREQ* packet passes to an intermediate node, it may forward the *RREQ* packet or prepare a routing reply *RREP* (Route Reply) package if there is an effective route to the destination in the cache. (*SId*, *BId*) is needed for the verification to avoid the *RREQ* received repeatedly. Each intermediate node records the node address and its *BId* of the last node when a *RREQ* packet is transmitted. Nodes also use timer to associate each record, which is used to delete the *RREQ* packets without receiving any reply prior to expiration.

When a node receives *RREP* packet, the corresponding information of the previous node is saved as the next hop of the forward packet and the destination node which plays the "forward indicator" role of the destination node. By doing so, each node only needs to store the information of the next-hop while all the relay nodes on the path are stored in the source routing.

The Figure 1 is given to illustrate the routing discovery scheme of AODV protocol in. Assume that the node *A* wants to transmit data packets to the node *G*, but there is no routing to node *G* in the cache, then the node *A* will broadcast a *RREQ* packet to all neighbors node (*B*, *C* and *D*) to initialize a route discovery process, all the *SId*, *DId*, *SSeq*, *DSeq*, *BId* and *TTL* are encapsulated in the *RREQ* packets, when the *RREQ* packet gets to the node *B*, *C* and *D*, these nodes find the routing cache immediately, if without the routing of node *G*, they forward the *RREQ* to neighboring nodes, or compare the *RREQ DSeq* and the *DSeq* in the cache, if *DSeq* of intermediate nodes is large, a *RREP* packet containing a routing to the destination node is given to source nodes. In Figure 2, there is a path to *G* in the cache of node *C*, and whose *DSeq* is greater than that of *RREQ* packets, node *C* transmits a *RREP* packet to source node *A*, the path *A-C-F-G* is stored in node *A*, and there will be *RREP* returned from the destination node, such as *A-B-E-G*, the relay nodes on the path choose the latest *DSeq* in *RREP* packet to update their routing table.

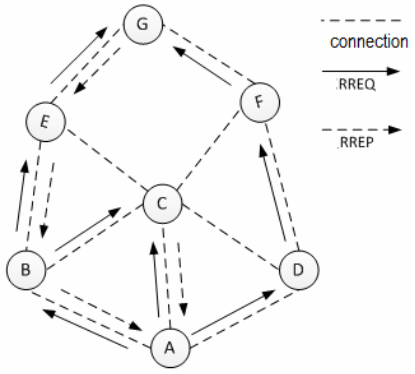


Figure 1. AODV route discovery

Route maintenance. When a node find a link is destroyed (by the link layer to confirm or HELLO information), it broadcasts a *RERR* packet (similar to the way DSR) to notify the source nodes and destination nodes. The process is shown in Figure 2. If the node link of *C* and *F* on the path *A-C-F-G* is destroyed, *C* and *F* transmit *RERR* packets to notify the source node and the destination node.

The main advantage of AODV is to reduce routing overhead. Another characteristic of AODV is to use extension ring search to control the flooding of *RREQ* packets. In addition, the use of the destination sequence number allows nodes to have more updated

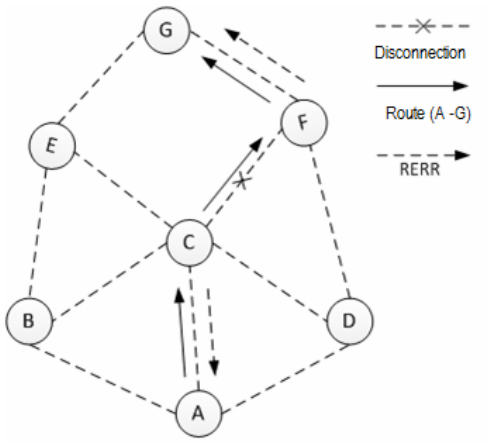


Figure 2. AODV route maintenance

routing. However, we should pay attention to several points when using AODV. First, it requires a two-way link and periodic link confirmation to detect link damage. Second, it needs to maintain the routing table. However, this flooding scheme might cause some security issues. Flooding attacks generated excessive traffic to lead to denial of service in MANETs [21].

3.2 Secure AODV

SAODV (Secure AODV) is an extension of the AODV routing protocol, used to protect routing discovery and provide security features, such as integrity, authentication and non-repudiation [22]. SAODV assumes that each node has got the signing secret key pair from the asymmetric encryption algorithm. Moreover, every node could verify the relations between address and public key of the other nodes. SAODV needs key management scheme and there are two mechanisms used to ensure the security of AODV messages:

(1) Digital signatures: make sure that the message has not been tampered with.

(2) Hash chain: ensure the security of variable hop in the message.

Authentication could be performed in the form of point to point for the immutable information, but that is not available for the variable information. It really doesn't matter which node initiate or forward routing error message, but instead adjacent nodes notifying the other nodes that could not be routed to a destination. Therefore, any node (initiate and forward routing error message) sign for *RERR* packet with a digital signature, any adjacent nodes received *RERR* packet verify the signature.

The extensible formats of *RREQ* and *RREP* including:

< *type, length, Hash function, maximum hop count, the top Hash, signature, Hash* >

The extensible formats of *RERR* including:

< *type, length, retain, signature* >

SAODV Hash chain. Hash chain is used to detect the integrity of *RREQ* and *RREP* messages hop. By running the one-way Hash function to form the Hash chain.

Every time one node initializes a *RREQ* or *RREP* messages, it performs the following operations [22]:

Generate a random number (seed).

Set the maximum hop count *Max_Hop_Count* as the survival time *TTL*.

$$Max\_Hop\_Count = TTL \quad \textbf{(1)}$$

Set Hash as the seed value.

$$Hash = seed \quad \textbf{(2)}$$

Set up the Hash function to be used

Table 1. Value of the Hash Function Domain

Value	Hash functions
0	Remain
1	MD5HMAC96
2	SHA1HMAC96
3-127	Remain
128-255	Relevant to the reality

Calculate *Top_Hash* through the seed and *Max_Hop_Count*

$$Top\_Hash = h^{Max\_Hop\_Count}(seed) \quad \textbf{(3)}$$

In which, *H* is a Hash function. *hi (x)* is the result running function h i times based on parameter x.

Whenever a node receives message of *RREQ* or *RREP*, it performs the following operations to verify the hop.

Hash function *h* is used to calculate Hash value *Max_Hop_Count* minus the value after Hash operations *Hop_Count* times, verifying whether the result is equal to the top of the Hash value.

$$Top\_Hash = h^{Max\_Hop\_Count - Hop\_Count}(Hash) \quad \textbf{(4)}$$

The node calculates new Hash value using Hash function before broadcasting *RREQ* or forwarding *RREP* again.

$$Hash = h\ (Hash) \quad \textbf{(5)}$$

SAODV digital signature. SAODV used asymmetric encryption, such as RSA for digital signature certification. The node used the only private key signature information first, and then uses the public key that all nodes have to decrypt while the node receives encrypted signature. The demonstration is given below to illustrate RSA digital signature process.

(1) Choose two large prime numbers first, such as p = 13, q = 11;

(2) Calculate $n = p * q$ = 143, $z = (p - 1) * (q - 1)$ = 120;

(3) Choose a random private key d = 19 that co-prime of z;

(4) Assume e as the public key, require $e * d$ mod z

= 1, choose e = 139;

When the node A likely transmits data to the node B, assuming the data of 3, 4, 1. A signature using the private key d and n, and the digital signature is: 81 (3^{19} mod 143), 69 (4^{19} mod 143), 1 (1^{19} mod 143). B uses the public key e and n to decrypt when it receives the signature, 3 (81^{139} mod 143), 4 (69^{139} mod143), 1 (1^{139} mod 143).

3.3 Performance Analysis

As there is no any secure scheme, AODV may be attacked by malicious nodes, compromised nodes and selfish nodes. Malicious nodes refer to the nodes that the attacker could not verify the legality of its own identity because the lack of effective encryption information; compromised nodes refer to the nodes that internal attackers could verify their identity as legal node and be trusted by other nodes, and that would launch an offensive within the network; selfish nodes refer to the nodes that tend to deny its own resources to make the other nodes could not benefit from it so as to save their own resources.

Message tampering attacks. An attacker could change the content of the routing messages, for instance, while forwarding RREQ, an attacker could reduce the hop count to increase the probability chosen for routing, so that it could analyze the communication between source node and destination node. One aim of this attack is to increase the destination sequence number to make the other nodes believe that the routing is the latest. The simulation results show that, in some scenarios, an attacker could discard 75% of packets by manipulating the destination sequence number.

Message discarding attacks. The attacker and selfish nodes could selectively discard (or all) the routing and data information. Because in MANETs, all mobile nodes could be used as terminal nodes or routing nodes, so this attack will lead the network paralyzed completely with the increase in the number of discarded messages.

Message replay (wormhole) attacks. The attacker could make a retransmission of the eavesdropped message in different positions. One of the replay attacks is a wormhole attack. Wormhole attacker could uses private channel to transfer RREQ directly to the destination node. Because wormholes attackers may not increase jump number, which will prevent other routing from being found. Wormhole attack could be combined with information discarding attack to prevent destination nodes to receive packets.

Therefore, the security requirements of AODV are as follows:

(1) Source authentication: ensure the correctness of node identity.

(2) Adjacent nodes authentication: the receiving nodes need to be able to determine the identity of the transmitting nodes.

(3) Message integrity: validate the routing information not be tampered with.

(4) Access control: ensure that the mobile nodes attempting to access the network have appropriate access permissions.

SAODV ensures the security of AODV by adding encryption arithmetic (Hash chain and digital signature).

4 Energy-efficient Secure AODV

The use of RSA digital signature in SAODV is to guarantee the data is not tampered, and the use of Cyclic Redundancy Check (CRC) could also achieve this goal. CRC is a kind of error detection code, which usually used for detecting the unexpectedly data change in storage devices or Internet. Data uses CRC algorithm to get a check code, this code attached at the back of the original data is transferred with the original data, then the receiver reuses the same CRC algorithm to check whether the data been tampered with. Popular representation is that appends a piece of data behind the original data and make sure that could be divided exactly by specific values.

The shortest key of RSA digital signature is for 1024-bit, the polynomial of CRC-4 is 5 bit. In addition, the computational complexity of CRC is much lower than that of RSA digital signature. So, we propose an Energy-efficient secure AODV protocol, which could effectively reduce the storage space and energy consumption of SAODV protocol, increase energy efficiency by using CRC instead of RSA digital signature to test whether the data has been changed.

4.1 Theoretical Derivation

Principal algorithm. Any binary strings could be written as a polynomial with coefficients of 0 or 1, for example: code "1101" could be written as polynomial "$x^3+x^2+x^0$". Accordingly, polynomial "$x^4+x^1+x^0$" could be written as code "10011".

The length of raw data is K, the polynomial of original data is set to $m(x)$, the length of check code for R, then the polynomial $g(x)$ is generated with $R + 1$ bits:

The division of formula (6) is die second division, that is, the highest power of the divisor and dividend is aligned, doing exclusive or calculation; In which, move $m(x)$ left to R places to get $M(x)$ times x^R, so as to empty out CRC check code for R places; $r(x)$ is the remainder that is CRC check code.

Attach the gotten CRC check code at the back of the next original data and then make a transmission together, the receiver divide the data by $g(x)$, and it represents the data has not been tampered with when there is no remainder.

$$\frac{m(x)\cdot x^R}{g(x)} = q(x) + \frac{r(x)}{g(x)} \quad \textbf{(6)}$$

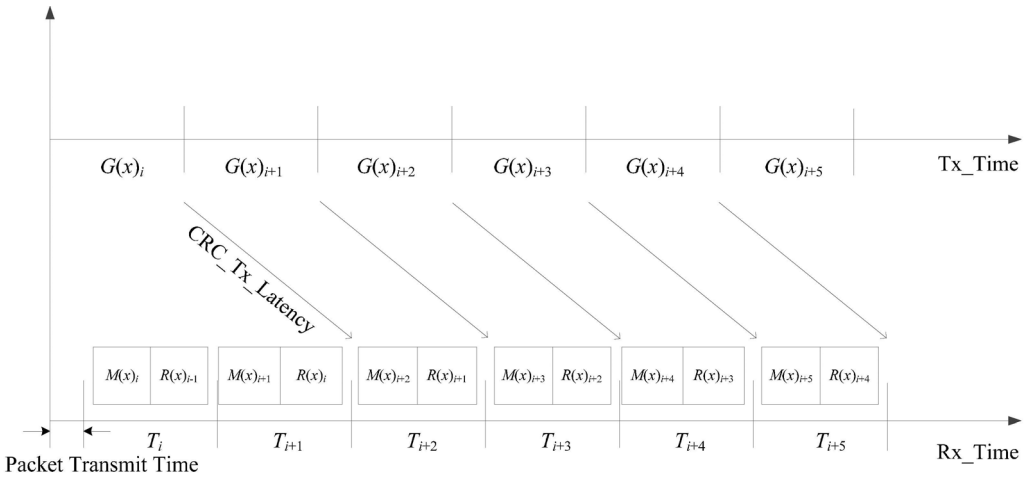


Figure 3. CRC tamper-proof scheme

4.1.2 CRC Tamper-proof Mechanisms

Generally, the error caused by natural factors such as interference or harass could use the CRC scheme detect the data which has been altered effectively, though if data is artificially manipulated and the CRC is changed at the same time by malicious nodes, it could not be detected whether the data has been tampered with the scheme of CRC.

In order to defend the tamper attack, we would like to generate pseudorandom polynomials. Usually the polynomial generated by CRC is a kind of fixed form, so that malicious nodes could tampered with the data and CRC easily at the same time, while if we use pseudorandom polynomials, it could reduce the possibility of tampering with the data and CRC. The transmitter and the receiver only need to make an appointment about the sequence of the using of the polynomial generate by pseudorandom in advance. In addition, we could use broadcast authentication protocol μTESLA to release the secret key later, the transmitting of CRC latency once, and let the data and the corresponding CRC transmit separately, reduce the possibility of malicious nodes tampering with the data and CRC at the same time. Principle as shown in Figure 3, the transmitter uses the generated polynomial $G(x)_i$ to calculate $R(x)_i$ when it transmits data $M(x)_i$, and transmit the last calculated $R(x)_{i-1}$.The receiver could receive the $R(x)_i$ and check the authenticity of the data using the generated polynomial $G(x)_i$ on a single latency.

4.1.3 Low Complexity Verification and Delayed Transmitting Mechanism

In a sense, the entire points of using RSA digital signature and CRC are both to guarantee the data not to be tampered. Although CRC is sample, and its security strength is not as RAS, Compared with RAS digital signature (1024 bytes), CRC (4 bytes) has certain advantages in computation and transmitted energy consumption, especially for resource-constrained nodes. Then, how to guarantee the integrity of CRC becomes critical issue. In this sub-section, we give the low complexity verification and delayed transmitting scheme to solve above problem, and use checksum for CRC code to guarantee its integrity to a certain extent. In order to illustrate proposed algorithm, the notations we have introduced and will introduce later are summarized in Table 2.

Table 2. Summary of notations

Notation	Definition
S_ID	Source node ID
D_ID	Destination node ID
BSN	Block sequence number
Len	Length of original packet
Payload	Payload of packet
CHK	Checknum for CRC
CRC	Cyclic Redundancy Check for original packet
$N_{Interval}$	Interval of transmission
P_buffer	Transmitting/Receiving packets buffer
C_buffer	Transmitting/Receiving CRCs buffer
Tx_packet	Transmitted packet (involved: packet, *CHK* and *CRC*)
Rx_packet	Received packet (involved: packet, *CHK* and *CRC*)

Briefly, the proposed scheme mainly involves two parts: generating CRC and delayed transmitting based on given transmission interval. In the E-SAODV, we give a structure of typical data packet is shown in Figure 4. Meanwhile, we claim that intermediate nodes only forward packets.

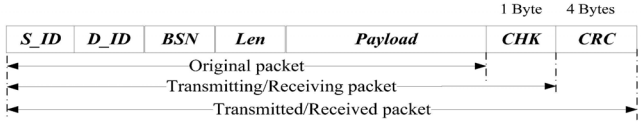


Figure 4. Structure of Typical Data Packet in E-SAODV protocols

The pseudo-code of DTM for source node is described in Algorithm 1.

Algorithm 1. DTM Algorithm for Source Node (In this case, $BSN_{max} = 65535$)

1: Construct two buffers: *P_buffer* and *C_buffer*;
2: Set *BSN*, *S_ID* and *D_ID*
3: Obtain original data (payload), calculate *Len*, construct original packet.
4: Generate *CRC*, and put it into *C_buffer[BSN+ $N_{Interval}$]*
5: Calculate the checksun of *CRC*, get *CHK*
6: Construct Transmitting packet, put it into *P_buffer[BSN]*
7: Construct *Tx_packet* from *P_buffer[BSN]* and *C_buffer[BSN]*
8: Transmit *Tx_packet*
9: Set (*BSN* +1) mod 2^{16} to *BSN*
10: Go to step 3

The pseudo-code of DTM for destination node is described in Algorithm 2.

Algorithm 2. DTM Algorithm for Destination Node

1: Obtain *Rx_packet,* resolve *BSN*, receiving packet and *CRC*,
2: Put receiving packet into *P_buffer[BSN]*, and put CRC into *C_buffer[BSN]*
3: Get the old receiving packet from *P_buffer[BSN- $N_{Interval}$],* resolve *CHK,* generate *old _CRC*
4: **if** CHK is the checksum of current *CRC* **then**
5: **if** *old _CRC* is equal to current *CRC* **then**
6: the receiving packet is valid and integrated.
7: **else**
8: the receiving packet is discussed.
9: **end if**
10: **else**
11: the receiving packet is discussed.
12: **end if**

4.2 Simulation and Analysis

Simulation analysis is performed using Network Simulator (NS-2), which most known tool for simulation of network scenarios and topologies. We simulated AODV, SAODV and E-SAODV protocol, made a comparison in terms of energy consumption, throughput and BPUE (Bits Per Unit of Energy). BPUE is a multi-parameter joint evaluation metrics based on the transmission distance and modulation level [23]. The simulation parameters are shown in Table 3.

Table 3. Simulation parameters

Parameter	Value
Number of nodes	50
Initial energy of nodes (J)	2
Simulation area (m^2)	1000*1000
Node movement speed (m/s)	0
Simulation time (s)	800
Transmission range(m)	250
Antenna Type	Omni antenna
Mobility Model	Random Way Point

The energy consumption of the three kinds of protocol is compared in Figure 5. It could be seen from the diagram that the AODV protocol has the largest energy consumption, the network energy consumption tends to be constant at about 700 s, which means that most of the nodes are energy depletion, network stops working; SAODV protocol has the minimum energy consumption, SAODV and E-SAODV deal is still in a rising state in the 800s, which means that the nodes have residual energy, the network could continue working.

The throughput of the three kinds of protocol is compared in Figure 6. It could be seen from the diagram that the throughput of AODV protocol is the biggest at about 700 s, and the throughput is no longer up due to stopping working of network. The throughput of SAODV protocol is the minimum.

Since AODV protocol has no any secure scheme, the operating speed is the fastest and the energy consumption and throughput of it is the largest; Instead, SAODV protocol joins the secure scheme, more complicated than the E-SAODV protocol, therefore it has the minimum energy consumption and throughput. The energy consumption and throughput of E-SAODV protocol is between AODV and SAODV protocol. It could be concluded from the Figure 5 and Figure 6: E-SAODV protocol is to reduce energy consumption by average of 35% in terms of SAODV when they have the same throughput.

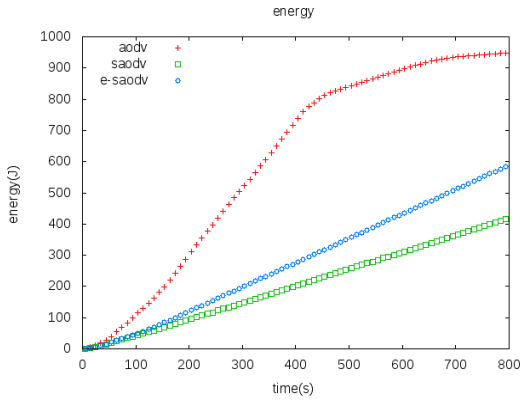


Figure 5. Energy Consumption of AODV, SAODV and E-SAODV

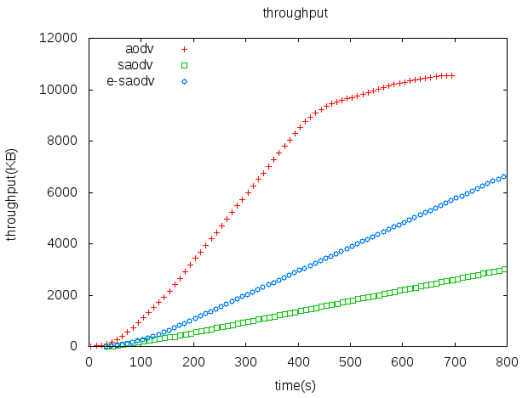


Figure 6. Throughput of AODV, SAODV and E-SAODV

BPUE of the three kinds of protocol is compared in Figure 6. It could be seen from the diagram that AODV protocol has the biggest BPUE while SAODV has the minimum; the BPUE of E-SAODV is between AODV and SAODV protocol. It could be seen from the figure that the BPUE index is about 60% higher than that of SAODV protocol when it remains steady, E-SAODV protocol. Figure 7 confirmed our view that E-SAODV protocol improves the energy efficiency of SAODV.

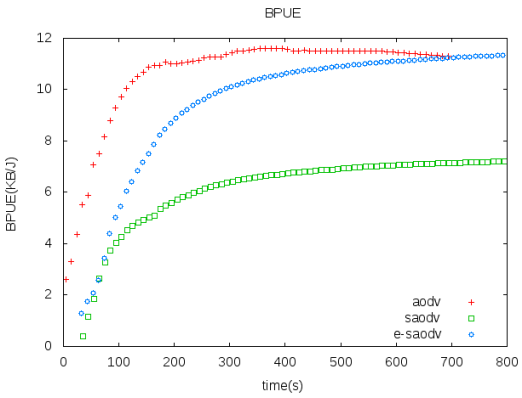


Figure 7. BPUE of AODV, SAODV and E-SAODV

5 Conclusions

Industrial sensor network is a special field of sensor network. As its internal architecture continuously extending in different directions due to its instrumentation and private network, the technology is different from that of sensor network. It also supports huge amounts of data and requires much attention at large in addition to the technical features of highly heterogeneous nature. This is the industrial application domain of the sensor network, usually has higher technical requirements, operational risk and financial return, these characteristics determine that the industrial sensor network has higher requirements on security than traditional sensor network, that is, Industrial WSN has a higher standard than traditional sensor network in the security architecture, network security technology, the potential risk of intelligent equipment, privacy protection, security management and guarantee measures. In this paper, E-SAODV protocol is proposed combining with industrial sensor network application scenarios based on SAODV protocol. Using cyclic redundancy check instead of digital signature could reduce the complexity of protocol and improve the energy efficiency of the protocol, furthermore, the tamper-proof of information is guaranteed by latency strategy of CRC in information domain. The simulation results show that the energy consumption is about 35% lower and BPUE index is about 60% higher in E-SAODV protocol than SAODV protocol. Meanwhile, the mechanisms of increasing energy efficiency and information tamper-proof could be used in the improvement of other AODV protocols. Finally, the better throughput could meet the requirement of the application in the industrial field.

Acknowledgement

This work is partially supported by the National Natural Science Foundation of China (61471346, 51404258), the Shanghai Natural Science Foundation (17ZR1429100), the Science and Technology Innovation Program of Shanghai (17511105903, 17DZ1200302), the NSFC-Shanxi Provincial People's Government Jointly Funded Project of China for Coal Base and Low Carbon (U1510115), the Natural Science Foundation of Qinghai province (2016-ZJ-922Q), the Science and technology project of Housing Urban and rural construction in Shandong Province (201419, 2015RK030), the Security production science and technology development plan of Shandong Province (201409, 201417), the independent innovation projects of Ji'nan University (201401210), the state administration of work security accident prevention technology project (shandong-0006-2014AQ, shandong-0001-2014AQ) and Project funding for young teachers of higher education in Shandong Province.

References

[1] C. Zhu, L. T. Yang, L. Shu, V. C. M. Leung, T. Hara, S. Nishio, Insights of Top-k Query in Duty-Cycled Wireless Sensor Networks, *IEEE Trans. on Industrial Electronics*, Vol. 62, No. 2, pp. 1317-1328, February, 2015.

[2] C. Zhu, V. C. M. Leung, X. Hu, L. Shu, L. T. Yang, A Review of Key Issues that Concern the Feasibility of Mobile Cloud Computing, *IEEE International Conference on Cyber, Physical and Social Computing*, Beijing, China, 2013, pp. 769-776.

[3] K. Wang, Y. Shao, L. Shu, Y. Zhang, C. Zhu, Mobile Big Data Fault-tolerant Processing for eHealth Networks, *IEEE Network*, Vol. 30, No. 1, pp. 36-42, January, 2016.

[4] L. Shu, L. Wang, J Niu, C. Zhu, M. Mukherjee, Releasing Network Isolation Problem in Group-Based Industrial Sensor

Networks, *IEEE Systems Journal*, Vol. No. 99, pp. 1-11, October, 2015.

[5] Y. Liu, H. Wang, J. Wang, K. Qian, N. Kong, K. Wang, Y. Shi, L. Zheng, Enterprise-Oriented IoT Name Service for Agriculture Product Supply Chain Management. *International Conference on Identification, Information and Knowledge in the Internet of Things*, Beijing, China, 2014, pp. 237-241.

[6] C.-H. Ou, Mobile Anchor-Assisted Localization for Mobile Sensor Networks, *Journal of Internet Technology*, Vol. 12, No. 1, pp. 37-48, January, 2011.

[7] T. Liu, X. Gao, L. Wang, Study on Multi-objective Optimization of Oil Production Process, *11th World Congress on Intelligent Control and Automation*, Shenyang, China, 2014, pp. 1824-1829.

[8] J. Moyne, M. Yedatore, J. Iskandar, P. Hawkins, J. Scoville, Chamber Matching Across Multiple Dimensions Utilizing Predictive Maintenance, Equipment Health Monitoring, Virtual Metrology and Run-To-Run Control, *5th Annual SEMI on Advanced Semiconductor Manufacturing Conference,* Saratoga Springs, New York, NY, 2014, pp. 86-91.

[9] J Gan, N. N. Xiong, H. Wen, Analysis of SCTP Concurrent Multipath Transfer in Vehicular Network Communication, *Journal of Internet Technology*, Vol. 16, No. 3, pp. 495-504, June, 2015.

[10] D. Dujovne, T. Watteyne, X. Vilajosana, P. Thubert, 6TiSCH: deterministic IP-enabled industrial internet (of things), *IEEE Communications Magazine*, Vol. 52, No. 12, pp. 36-41, December, 2014.

[11] N. Gandhewar, R. Patel, Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network, *Fourth International Conference on Computational Intelligence and Communication Networks*, Mathura, Uttar Pradesh, India, 2012, pp. 714-718.

[12] S. P. S. Tomar, B. K. Chaurasia, Detection and Isolation of Sinkhole Attack from AODV Routing Protocol in MANET, *International Conference on the Computational Intelligence and Communication Networks*, Udaipur, Bhopal, MP, India, 2014, pp. 799-802.

[13] K. Xiong, M. Yin, W. Li, H. Jiang, A Rank Sequence Method for Detecting Black Hole Attack in Ad Hoc Network, *International Conference on Intelligent Computing and Internet of Things*, Harbin, China, 2015, pp. 155-159.

[14] A. Gupta, Mitigation Algorithm Against Black Hole Attack Using Real Time Monitoring for AODV Routing Protocol in MANET, *2nd International Conference on Computing for Sustainable Global Development*, New Delhi, India, 2015, pp. 134-138.

[15] U.-H. Syed, A.I. Umar, F. Khurshid, Avoidance of Black hole affected routes in AODV-based MANET, *International Conference on Open Source Systems and Technologies*, Lahore, Pakistan, 2014, pp. 182-185.

[16] C. E. Perkins, E. M. Royer, Ad-hoc On-demand Distance Vector Routing, *IEEE Second Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, 1999, pp. 90-100.

[17] P. Jain, A. Suryavanshi, Energy Efficient Local Route Repair Multicast AODV Routing Schemes in Wireless Ad hoc Network, *International Conference. on Advanced Communication Control and Computing Technologies*, Tamilnadu, India, 2014, pp. 1168-1173.

[18] A. Joshi, R. Kaur, A Novel Multi-cast Routing Protocol for VANET, *IEEE International Advance Computing Conference*, Bangalore, India, 2015, pp. 41-45.

[19] B. Bansal, M.R. Tripathy, D. Goyal, M. Goyal, Improved Routing Protocol for MANET, *Fifth International Conference on Advanced Computing & Communication Technologies*, Rohtak, Haryana, India, 2015, pp. 340-346.

[20] P. Ranjan, R. L. Velusamy, Optimized Local Route Repair and Congestion Control in Mobile Ad Hoc Network, *International Conference on Computing & Communications Technologies*, Chennai, India, 2015, pp. 328-333.

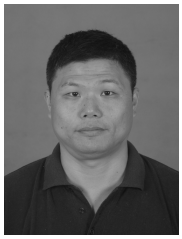
[21] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, D. Gaiti, Flooding Attacks Detection in MANETs, *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications*, Shanghai, China, 2015, pp. 1-6.

[22] M. G. Zapata, Secure Ad Hoc On-demand Distance Vector Routing, *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol. 6, No. 3, pp. 106-107, March, 2002.

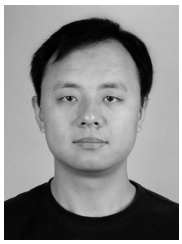
[23] W. Fang, Z. Shi, L. Shan, F. Li, Y. Xiong, A Multi-parameter Joint Evaluation Scheme in Energy Consumption for Wireless Sensor Networks, *Chinese High Technology Letters*, Vol. 25, No. 8-9, pp. 753-759, October, 2015.

Biographies

Weidong Fang is a Ph.D. and an associate professor in Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences, Shanghai, China. Currently, his research interests are information security in wireless sensor network & mobile Ad hoc network, including trust management, secure network coding and secure routing protocol.



Chuanlei Zhang received the Ph.D. degree in electrical engineering from China University of Mining and Technology (Beijing), Beijing, China in 2006. He is currently an associated professor in the School of Computer Science and Information Engineering at Tianjin University of Science and Technology. His research interests include Pattern Recognition and Artificial Neural Network, Data Mining, Wireless Communication, Multimedia Retrieval and Video Content Analysis and applications in Bioinformatics, Finance.



Wei Chen received the Ph.D. degree in communications and information systems from China University of Mining and Technology, Beijing, China, in 2008, and he joined the School of Computer Science and Technology, China University of Mining and Technology at Xuzhou, where he is currently an associate professor. His research interests include Intelligent Information Processing, Wireless Communications, Big Data and Cloud Computing.

Ming Li received the B.S. degree from the Yangzhou University of China, Yangzhou, in 2005 in electrical engineering, and received the Ph.D. degree with the School of Mechanical Electronic & Information Engineering, China University of Mining & Technology, Beijing, in 2011. Her research interests include wireless communication and information system.

Fengying Ma received the Ph.D. degree in communications and information systems from China University of Mining and Technology, Beijing, China, in 2009, and she joined the School of Electrical Engineering and Automation, Qilu University of Technology at Jinan, where she is currently a professor. Her research interests include Intelligent Control, Intelligent Information Processing, Wireless Communications, Big Data and Cloud Computing.