Industrial Wireless Sensor Network-Oriented Energy-Efficient Secure AODV Protocol

Weidong Fang[1], Chuanlei Zhang[2], Wei He[1(✉)], Wei Chen[3], and Fengying Ma[4]

[1] Key Laboratory of Wireless Sensor Network and Communication, Shanghai Institute of Micro-system and Information Technology, Chinese Academy of Sciences, Shanghai 201800, China
{weidong.fang,hewei}@mail.sim.ac.cn
[2] School of Computer Science and Information Engineering, Tianjin University of Science and Technology, Tianjin 300222, China
al7647@gmail.com
[3] School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China
chenw@cumt.edu.cn
[4] School of Electrical Engineering and Automation, Qilu University Technology, Jinan 250353, China
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 fields. Meanwhile, researches on AODV have very in-depth, whether in improving performance, or enhancing security. Unfortunately, there are few researches on joint energy efficiency and security. In this article, we propose an Energy-efficient Secure AODV Protocol (E-SAODV) in Industrial Wireless Sensor Network (IWSN). In E-SAODV, the low complexity verification and the Delayed Transmitting Mechanism (DTM) is proposed and applied. The mechanism involve two parts: the polynomial of the Cyclic Redundancy Check 4 (CRC-4) that substitutes the shortest key of RSA digital signature in SAODV guarantees the integrity of data verification, and reduces storage space, computation and energy consumption. DTM is implemented to separate the check code and valid data, and to achieves tamper-proof. The simulation results show that comprehensive performance of proposed E-SAODV is a trade-off the energy efficiency and security, and better than AODV and SAODV, and could meet the requirement of the throughput in the industrial scene.

Keywords: Industrial Wireless Sensor Network · Security · AODV · Energy efficiency

1 Introduction

As the emergence and development of Wireless Sensor Network (WSN) [1], Cloud Computing [2], Big Data [3] and intelligent terminal, Industrial Wireless Sensor Network (IWSN) [4] has become networking technologies to lead the trends in technology

J.-H. Lee and S. Pack (Eds.): QShine 2016, LNICST 199, pp. 406–415, 2017.
DOI: 10.1007/978-3-319-60717-7_40

development. IWSN is an interdisciplinary research, which involves automation, computer and communications. The requirements of IWSN mainly focused on the following fields: Localization [5], Optimization of Production Process [6], Equipment Monitoring and Maintenance [7] and so on.

Unfortunately, the particularity of the industrial environment makes application of IWSN have to consider some adverse factors: wireless signal multipath caused by reflection and scattering of large-scale equipment and metal pipes, 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 IWSN application is secure transmission of production process parameters. This is due to that network information security is facing a growing challenge. The possibility that control systems of industrial facilities are damaged by network intrusion does exist. 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 IWSN mainly involves information sensing security and network transmission security. Meanwhile, the low-power technology has been one of the hot topics [8]. In this paper, an Energy-efficient Secure AODV protocol is proposed to meet these requirements of defense attack and low-power in IWSN. The rest of this paper is organized as follows: in Sect. 2 a brief review of AODV and its evolution are given. The preliminary knowledge and analysis are represented in Sect. 3. The E-SAODV protocol is proposed, and simulation results and analyses of the proposed protocol are presented in Sect. 4. Finally, some concluding remarks are provided in Sect. 5.

2 Related Works

As a traditional routing protocol, AODV protocol has been a hot topic. At presented, research on AODV is divided into two categories: one is focus on enhancing its security; the other is improving its performances, such as reliability, transmission performance under dynamic topology, and so on.

2.1 Security Enhancement

As we all know, the design of AODV protocol does not take account for security. To meet different application requirements, various security schemes have been researched. These schemes mainly detect, defense or mitigate some specific attacks. In recent years, the studies have focused primarily on sinkhole attack, blackhole attack and Sybil attack.

Gandhewar and Patel proposed a mechanism for detection and prevention of Sinkhole Attack on the context of AODV protocol [9]. This mechanism of detection & prevention considered the behavior of sinkhole attack and AODV working, which mainly consist of four phases as Initialization Phase, Storage Phase, Investigation Phase, and Resumption Phase. The mechanism could improve the performance of

AODV under sinkhole attack. Tomar and Chaurasia put forward the mechanism of detection and isolation of sinkhole attack [10]. The key point of this mechanism 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. 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 [11].

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

2.2 Performance Improvement

AODV is a distance vector routing protocol [12]. It supports intermediate nodes reply, make source node quickly obtain routing, and effectively reducing the number of broadcast. Since 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, performance improvements of AODV mainly involve in the following areas: Energy efficiency, improving throughput, load balancing and so on, especially, in the industrial scene.

Jain and Suryavanshi proposed a new maximum energy Local Route Repair (LRR) approach with multicast AODV routing protocol [13]. These schemes included two processes: establishing path and forwarding packets from source node to destination node. 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 facilitated communication among vehicles through RSUs (Road-Side Units) and broadcasted in nature. They discussed prediction based 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 [14].

From above analysis, enhancing security and 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 and Analysis

3.1 AODV

AODV is a source driven routing protocol [12], 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 wireless sensor network, the AODV protocol could also be used in the wireless 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 AODV protocol involves two phases: route discovery and route maintenance.

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. 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 mechanism and there are two mechanisms used to ensure the safety of AODV messages:

- Digital signatures: make sure that the message has not been tampered with.
- Hash chain: ensure the safety 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.

1. 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:
   (1) Generate a random number (seed).
   (2) Set the maximum hop count *Max_Hop_Count* as the survival time *TTL*.
   (3) Set Hash as the seed value.
   (4) Set up the Hash function to be used
   (5) Calculate *Top_Hash* through the seed and *Max_Hop_Count*

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.

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

2. 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 $e * d \bmod z = 1$, choose $e = 139$.

3.3 Performance Analysis

As there is no security mechanism, AODV may be attacked by malicious nodes, compromised nodes and selfish nodes.

1. 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.
2. Message discarding attacks
   The attacker and selfish nodes could selectively discard (or all) the routing and data information. Because 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.
3. 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.

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

4 Energy-Efficient Secure AODV Protocol

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

1. 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.

2. CRC Tamper-proof Mechanisms
   Generally, the error caused by natural factors such as interference or harass could use the CRC mechanism 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 mechanism 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. 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.

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 mechanism to solve above problem, and use checksum for CRC code to guarantee its integrity to a certain extent.

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 agreement, 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 [15]. The simulation parameters are shown in Table 1:

Table 1. 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 agreement is compared in Fig. 1. 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 agreement has the minimum energy consumption, SAODV and E-SAODV deal is still in a rising state in the 800 s, which means that the nodes have residual energy, the network could continue working.

The throughput of the three kinds of agreement is compared in Fig. 2. It could be seen from the diagram that the throughput of AODV protocol is biggest at about 700 s, and the throughput is no longer up due to stopping working of network; The throughput of SAODV agreement is the minimum.

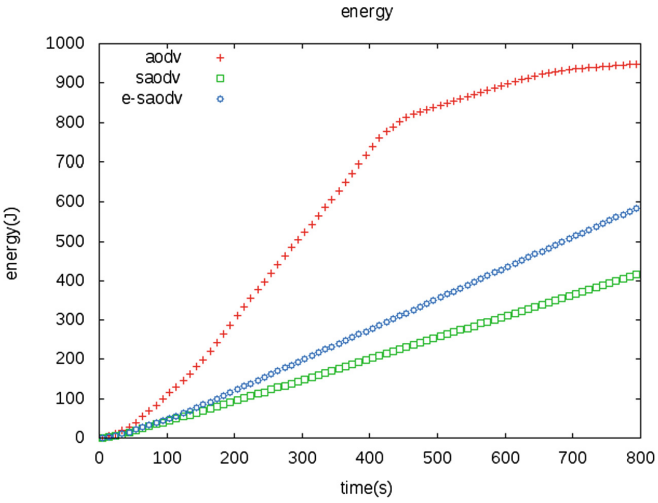

Fig. 1. Energy consumption of AODV, SAODV and E-SAODV protocols

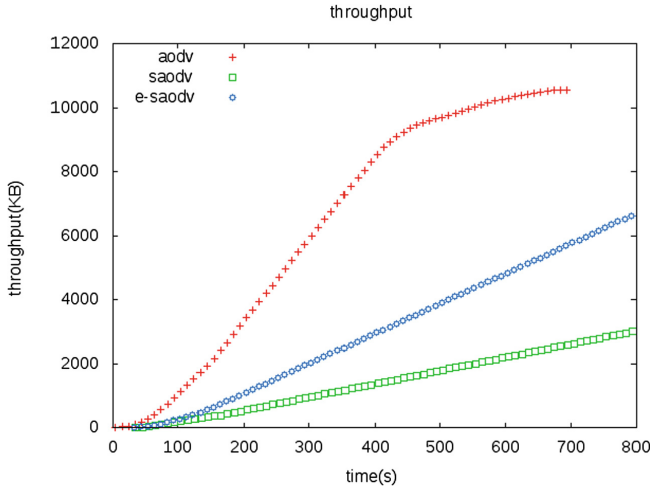

Fig. 2. Throughput of AODV, SAODV and E-SAODV protocols

As AODV protocol has no security mechanism, the operating speed is the fastest and the energy consumption and throughput of it is the largest; Instead, SAODV agreement joins the security mechanism, more complicated than the E-SAODV agreement, therefore it has the minimum energy consumption and throughput. The energy consumption and throughput of E-SAODV agreement is between AODV and SAODV protocol. It could be concluded from the Figs. 1 and 2: E-SAODV agreement is to reduce energy consumption by average of 35% in terms of SAODV when they have the same throughput.

5 Conclusions

Industrial WSN is a special field of Wireless Sensor Network, with the internal architecture continuously extending in different directions based on instrumentation and private network as basic components, its own technology therefore may be different from the general of the Wireless Sensor Network. Industrial WSN also gives a higher request to safety in addition to the technical features of highly heterogeneous, huge amounts of data. This is the industrial application domain of the Wireless Sensor Network, usually has higher technical requirements, operational risk and financial return, these characteristics determine that the Industrial WSN has higher requirements on security than traditional Wireless Sensor Network, that is, Industrial WSN has a higher standard than traditional Wireless Sensor Network in the security architecture, network security technology, the potential risk of intelligent equipment, privacy protection, safety management and guarantee measures. In this paper, E-SAODV protocol is proposed combining with Industrial WSN application scenarios based on SAODV agreement. Use cyclic redundancy check instead of digital signature to reduce the complexity of agreement and improve the energy efficiency of the agreement, 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 agreement. At the same time, 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 scene.

References

1. Zhu, C., Yang, L.T., Shu, L., Leung, V.C.M., Hara, T., Nishio, S.: Insights of top-k query in duty-cycled wireless sensor networks. IEEE Trans. Ind. Electron. **2**, 1317–1328 (2015)
2. Zhu, C., Leung, V.C.M., Hu, X., Shu, L., Yang, L.T.: A review of key issues that concern the feasibility of mobile cloud computing. In: The IEEE International Conference on Cyber, Physical and Social Computing (CPSCom), pp. 769–776. IEEE Press, New York (2013)
3. Wang, K., Shao, Y., Shu, L., Zhang, Y., Zhu, C.: Mobile big data fault-tolerant processing for eHealth networks. IEEE Netw. **1**, 36–42 (2016)
4. Shu, L., Wang, L., Niu, J., Zhu, C., Mukherjee, M.: Releasing network isolation problem in group-based industrial wireless sensor networks. IEEE Syst. J. **10**, 1–11 (2015)
5. Luis, P., Francisco, A., Lorenzo, F., Oscar, R.: Performance of global-appearance descriptors in map building and localization using omni-directional vision. Sens. (Basel) **2**, 3033–3064 (2014)
6. Liu, T., Gao, X., Wang, L.: Study on multi-objective optimization of oil production process. In: The 11th World Congress on Intelligent Control and Automation, pp. 1824–1829 (2014)
7. Moyne, J., Yedatore, M., Iskandar, J., Hawkins, P., Scoville, J.: Chamber matching across multiple dimensions utilizing predictive maintenance, equipment health monitoring, virtual metrology and run-to-run control. In: The 25th Annual SEMI on Advanced Semiconductor Manufacturing Conference, pp. 86–91 (2014)

8. Dujovne, D., Watteyne, T., Vilajosana, X., Thubert, P.: 6TiSCH: deterministic IP-enabled industrial internet (of things). IEEE Commun. Mag. **12**, 36–41 (2014)
9. Gandhewar, N., Patel, R.: Detection and prevention of sinkhole attack on AODV protocol in mobile ad hoc network. In: The Fourth International Conference on Computational Intelligence and Communication Networks, pp. 714–718 (2012)
10. Tomar, S.P.S., Chaurasia, B.K.: Detection and isolation of sinkhole attack from AODV routing protocol in MANET. In: The International Conference on the Computational Intelligence and Communication Networks, pp. 799–802 (2014)
11. Xiong, K., Yin, M., Li, W., Jiang, H.: A rank sequence method for detecting black hole attack in ad hoc network. In: The International Conference on Intelligent Computing and Wireless Sensor Network, pp. 155–159 (2015)
12. Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: The Second Workshop on Mobile Computing Systems and Applications, pp. 90–100. IEEE Press, New York (1999)
13. Jain, P., Suryavanshi, A.: Energy efficient local route repair multicast AODV routing schemes in wireless ad hoc network. In: The International Conference on Advanced Communication Control and Computing Technologies, pp. 1168–1173 (2014)
14. Joshi, A., Kaur, R.: A novel multi-cast routing protocol for VANET. In: The IEEE International Advance Computing Conference, pp. 41–45. IEEE Press, New York (2015)
15. Fang, W., Shi, Z., Shan, L., Li, F., Xiong, Y.: A multi-parameter joint evaluation scheme in energy consumption for wireless sensor networks. Chin. High Technol. Lett. **8–9**, 753–759 (2015)