DOI: 10.21917/ijct.2021.0369

A RELIABLE FAST AND IDEAL TRAFFIC AWARE SECURE ROUTING PROTOCOL BASED ON MULTI-HOP CROSS SITE LEAPING FOR EFFICIENT PACKET TRANSMISSION IN WSN

A. Ambeth Raja[1] and A. Udhaya Kumar[2]

[1]Department of Computer Applications, Thiruthangal Nadar College, India
[2]Department of Computer Science, Agurchand Manmull Jain College, India

Abstract

Fast Transmission in Wireless medium possess on node selection routing and unicasting the wireless sensor networks of the traditional secure aggregation system, the node broadcast it to all its neighbors as compared to what it contained. However, due to the rigorous network environment surrounding the nodes, many researchers usually take a different approach from traditional networks. Wireless sensor networks (WSN) are currently used in a variety of applications and will be used in more applications in the future. However, wireless sensor networks tend to be more unreliable than wired networks. In this paper, proposes A Reliable fast and ideal traffic aware secure routing protocol (RTASR) based on multi-hop cross site leaping for efficient packet transmission in WSN. Group-based fast proximity detection algorithm (GBFA) solves these problems. By bearing neighboring information in the beacon pocket, the node knows some potential neighbors in advance. This allows fast discovery to pick up the most energy-efficient neighbors to speed up energy efficiency and reduce network communication load, and actively nodes to verify that this dynamic neighbor is a true neighbor. The simulated results show that the proposed scheme reduces the loss of bandwidth in comparison to routing mechanisms that extend the life of the network.

Keywords:

Traffic Aware Routing, Node Bouncing, Cross Site Verification, Multi Hop Verification, Data Collection, Secure Routing, Packet Flow

1. INTRODUCTION

Today, many of valuable data that can be considered confidential through the circulation of the network (budget, credit card number, marketing data, etc.), many. Security, because these data cannot be read or altered by a third party. It will be very important, human services that are provided are always available and only permitted (confidentiality, integrity, responsiveness) there to here. Wireless network security is the process of designing, implementing and ensuring the safety of wireless sensor networks. It includes coverage of wireless computer networks and network security is a subset. The communication medium, hackers' traffic/packets will not be able to see the content. The wireless network detection and prevention system also enables wireless network security by alerting wireless network administrators when a security breach occurs.

Populated tributary nodes in the WSN can collect information and/or analyze them more closely to preprocess base knots (sinks). The nodes themselves are forced to self-organize and adjust their behavior to the current network conditions resulting in frequent topological changes in the unmanned and are. The sensor is generally defined as the communication and computing power of only the power and memory knot.

The sensor communicates with the device, which can detect and cause damage. Fast, high-efficiency sensors can be improved and improved at the present time to improve energy consumption when designing sensors with less data during a weather challenge. Precautions must be taken against the attack. Broadcast information is often used by wireless sensor networks. These attacks can cause security flaws.

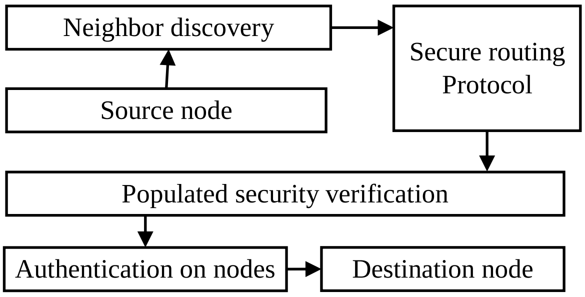

Fig.1 Process of secure data transmission in WSN

Security management and substantiation contrivances that recognize the sensor nodes to each other. By changing the location of a fixed topology, because you cannot create mobile sensor nodes need to be made secure routing.

Routing the security mechanism can be a complex problem, the security mechanisms cannot be simplified in terms of packet transitions power efficiency and computational complexity. The attacks now control the flow of data traffic is routed to the source and destination nodes. For example, packets can be sent, thus causing delays in non-optimal routes, or where they are missing, lost packets can be sent. In addition, an attacker could create network congestion routing loops. WSN will be able to reflect on the information gathered from network to network attacks to cause waves. We are security threats, intrusions and attacks, figures from the waves and knowing that they can help narrow safety data, safety-related data to define the data.

The development of this technology, security, architecture and protocol design issues need to address the challenges. Important wireless web network with state-of-the-art research, such wireless coverage, network capacity, manageability, and continues to prove that continue to be open to important issues such as network security. Various types of security data General WSN applications. Depending on the different diagnostic methods, the general feeling of safety data from certain data (e.g., received signal strength indicator, acknowledgment message, etc.), and other special data protection, there are some data (for example), but not specifically require a fingerprint to be extracted.

2. RELATED WORK

We, referring to security, there are a number of terms very important. Risk is defined as the accidental or the future of the exhibition of information as a result of the bad operation of the wrong design of the hardware or software [1]. Vulnerability indicates when the operation of the software and / or hardware component failure exposes system that penetrates. We start from here, it is possible to define the attack as an event for the excellent operation of the system, if it is successful, you will not be able to. If the attack is successful, we gain access to the file or program without detection or control is gained to the computer, we are dealing with penetration. Many WSN security protocols in the real-world applications on the main issue [2] [3]. This study focuses on the defense mechanisms of the two specific types of attacks that have occurred in the implementation of the network. Unwanted packets are sent to the service unavailable, so the services are being denied proper sensor nodes denial of service (DOS) attacks. Wireless sensor spots of storing sensitive information on rivals in an attempt to get the passive information gathering attacks [4].

WSN environment monitoring application in many fields and the environment is an integral part of the collected data. Large-scale, self-organizing, dynamic topology and tight resources, however, their unique characteristics of wireless sensor networks are very vulnerable to attack [5] [6]. It is proposed to effectively detect a variety of WSN attacks on numerous systems. Wireless Channel The key generation of years is a way to achieve confidentiality based on private key in the physical layer, using a wireless communication medium to create private key in public channel [7]. Wireless sensor networks can reduce network capacity and longevity and vulnerabilities to various malicious security attacks. This makes the cluster routing protocol with multiple nodes and cluster heads even more important [8] [9]. The idea is, through legitimate access point, you have to fool the part of the legitimate device to associate with this access point.

In order to enterprises and small and medium-sized enterprises to sustainable maintenance and competitiveness, it has become familiar with the benefits of a robust security platform. Intellectual property and proprietary information are a very valuable asset for these companies [10], it has penetrated into various fields of the national economy, such as health care, and closely are related to the daily life of people. Nevertheless, wireless network security, mainly in the following aspects, there still is one of the factors that hinder its popularity [11] [12]. In summary, the wireless network security problem, carriers, mobile node terminal, and is caused by release of dynamically changing network topologies. Security threats to the node terminal of the wireless network is mainly as follows. The attacker, via a wireless network in order to implement the attack, was connected to the attack of the network, seeking to implement management denial-of-service attacks, and the legitimate users, unauthorized access to network resources pretend wireless network control rights to the attack of the target network via [13]. By reducing, additional technology to enhance security and regular receiver, the security gap between the eavesdropping. Scrambled information bits SNR despite the still small value, and has a low bit error rate.

New technology, very little amount of such latency, such as the reduction of power consumption in the communication, there are a number of requirements [14] [15]. The detected malicious node is blacklisted by the sensor node, the proposed stop communication to and from the node / As, where not where protocol blacklist Safety [16]. For any wireless network technology, it has been considered one of the most important factors for security obtain a large approval. Method for detecting a variety of attack is studied intensively, have been reported in the literature, they none WSN in-depth on the collection and data analysis of security data to detect the mainstream of attack of the It does not provide a review [17].

Excellent choice and will computing power for the security physical layer to prevent much in eavesdropping attack for wireless sensor networks and energy [18]. However, some of them, routing consider to design a security mechanism from the system architecture view. The lack of a methodology for managing security be reliable. The complexity of the security requirements in a strange situation, will lead to the misplacement of duplication of security mechanisms and security features [19]. Network based security used in this form of speed and fast packet transition with verified hop, is a security gap, such as the many previous works, which is the maximum ambiguous used as a measurement for the security. The complexity of the calculations in cryptography, gives the advantage of physical layer security technology [20]. An attempt was made to achieve both of such reliability and security, such as the still high computing power and the probabilistic encryption and channel recognize and encryption requires energy, but there are several encryption technologies.

3. MATERIALS AND METHODS

With the increasing use of wireless communication in sensor networks, security issues in the network have become increasingly important and the focus of the present study has changed. Cybersecurity has always been the main focus of companies at the same time. However, many companies' current security systems have low accuracy and security situation predictions with longer response times. While new types of attacks, such as advanced persistent threats, continue to emerge, major threats are becoming the security of corporate networking. Experts such as cloud computing and big data informatics in many fields in recent years have begun trying to integrate these technologies into security environment awareness for enterprise networks. Due to the complexity of data dependencies in enterprise security data warehouses, traditional modeling methods affect the effectiveness of network security incident analysis to streamline data and meet the high requirements.

A Reliable fast and ideal traffic aware secure routing protocol based on multi-hop cross site leaping for efficient packet transmission in WSN. In order to achieve the above objectives and avoid network partitioning, parameters are taken into account at high residual power, link quality, constant, and minimum hops nodes in order to select the optimal path to the algorithm. Taking into account the above parameters can improve the security standard on route verification to improve network efficiently and balanced energy consumption.

As for the high residual energy, the high residual energy state would then drive the transport load after the node selection and extend the lifetime of the WSN. The Fig.2 shows the Ideal traffic aware secure routing on multi-hop cross site leaping (ITASR). By distributing network security analysis, it essentially involves the following steps: First, it should collect as much information as possible about the distribution network, including switching angles and voltage switches including the voltage swing, and second, the power outage including the current security status of the system security code. So, the sender can understand the state of the current system. Thirdly, the load forecast is predicted, based on the available data, as a benchmark for the future of the power house catalog, such as its current benchmark. It is the SA of the distribution network that analyzes the security analysis process. There are three stages that meet the definition. Therefore, the security SA is not the same. Basic content of the distribution network.

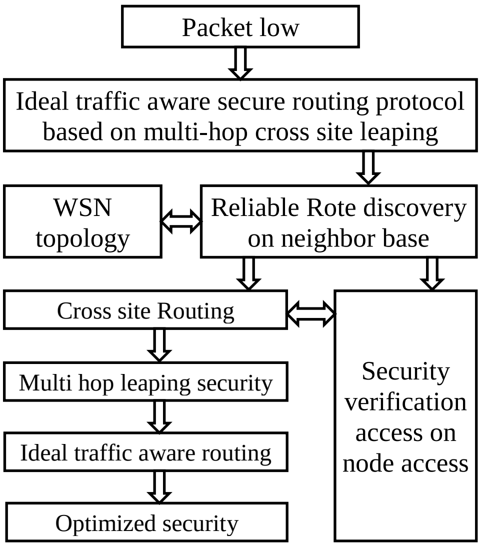
Packet low
Ideal traffic aware secure routing protocol based on multi-hop cross site leaping
WSN topology
Reliable Rote discovery on neighbor base
Cross site Routing
Multi hop leaping security
Ideal traffic aware routing
Optimized security
Security verification access on node access

Fig.2. Ideal traffic aware secure routing on multi-hop cross site leaping (ITASR)

3.1 CROSS SITE ROUTING

This cross-site routing turn reduces the energy consumption that the relay nodes extend to their network through packet verification protection; the aim is to minimize the use of control packets over wireless sensor networks. The proposed cross-layer verifier the recover site of transmission the route has been developed to provide information and analytics modeling to achieve these simulation results of the enterprise by optimizing energy consumption, demonstrating better performance and improved power efficiency in wireless sensor networks.

Algorithm: Cross Site Routing

```
Compute the $node_G$($Ver$ as $tras_n$ node, $Erf$ as $refrelect$ node),
Region cross route $R_{cs} = \{(v_{r1}, v_{r2}), (v_{r2}, v_{r3}),..., (v_{ri},v_{ri+1})\}$,
For generalize the node pf packet transmission for $js$=2 to $sr$ secondary
    Relay $J_s \rightarrow S$++ response node
    If ($j_s$ = 2 and $v_j$ packet access on relay authentication)
        Arrange node $v_r$ with the relay authentication
    Else
        Terminate ($v_j,v_{j+1},...,v_{si+1}$) to terminate
    End if
    For related hop access $h = s_r$ to $j_r$
        Allow the packet to transfer on relay node
        $R_l$++
        Alter mean time $T$ access
        Return $R_l \rightarrow G$;
    End For
End For
```

The DSR (distance vector Routing) protocol and routing algorithms include many beneficial routing protocol foundations. For example, when all nodes are almost static compared to each other, the DSR-sized path control packets overlap with the coordinate reaching zero. Similarly, if an intermediate node is unable to restart it, it immediately connects to the network at other points in the forward packets and does not significantly affect the routing. Therefore, the advantages are routing-based open source. DSR is primarily designed for ad hoc wireless networks with no self-organizing and self-configuring existing infrastructure or administration.

3.2 RELIABLE ACCESS NODE SELECTION

By the reliable protection on transmission node selection important with the presence of a few hostile nodes can lead to reconciliation of the paths, and as a result, the network has to rely on time and new routing innovation communication cycles. This imposes arbitrary delays before establishing a non-corrupted path, and imposes excessive transmission overhead on continuous broadcast requests. In particular, deliberately routing messages will eventually cause the node to experience a denial of service (DOS). This type of project vulnerability protects combatant and acquisition surface information. Target group of access node is given below:

$$T_g = (s+D)^n = \sum_{i=0}^{I++} \binom{n}{G} Hop^k RI^{n-k} \tag{1}$$

where *s* represents source *D* represented destination on the form of, *I* value node deployment for reliable access RL with K authentication using Group validation to secure the packet transmission.

These will send *M* packets with backpressure routers and random nodes associated with the site. The Back-Pressure Routing algorithm occurs when the traffic value from the current node is used to determine the next hop. In this way, our packets are routed with less congestion and faster transmission and this will result in fewer packets. Since time and time again, traffic at a particular stage is often considered a single node, because different paths have been taken

3.3 MULTI HOP LEAPING

The reactive routing protocol relies on a multiple hop transmission rating to transmit each packet. In directive to find a way out of a network, a reactive routing calculates the path and demands of the protocol and returns the path and floods the network. Using active protocols to navigate the sensor networks and refresh tables can be very costly as it can have very low data rates.

On the contrary, the reaction method is optimal in such cases. It is a communication environment where a large ad hoc network can be extended and mobile nodes are attached to the emergency system, usually working as a team and participating in a collaborative manner.

Algorithm: Multi-Hop Routing

```
Initialize network parameters NP on Route $MLhp$
Create regional group node List of Transmission Path
  If $MLhp \rightarrow G_{nl}$ == $exit$
    Create new random map region sector
    For each verifying packet flow Gnl-authentication
      Packet pt==allows sum of realy node
      Hop cout ++ as Gnl
      Return Gnl
    End For
    Verify the packet header passed by the $e_{ah}$ node relay on Hop
    Selective sink $S_t \rightarrow$Passes node Begins
    Check whether already node terminate access Packet
    If yes got reject and date route table Else
      Update the routing table Node resembles.
    End If
    If they compute the authentication on Hop Wait for the $T$ time
    for Node response Else
      If the packet is not destined for the current node to Jump
      close relay node,
          Check for the destination node
          Transmit the packet Group header
          Return Node passed
      End if
    End if
  End if
```

This effectively spreads information across mobile displays. This limits the discovery of low overhead routes in the area created by possible paths through the scope of route discovery packets. These methods are made possible by using bandwidth and location information. The packets are sent by reorganizing the controls using the path. Therefore, this algorithm is an excellent choice for parcel transmission in our network year.

3.4 IDEAL TRAFFIC AWARE ROUTING

The Traffic prediction is important for fast and efficient transmission, this Ideal traffic aware routing mainly designed for three types of qubits that transmit data and control the special relationship between qubits and qubits called flexibility arranged flexible quantum frames. Each displacement quantum group has a different quantum law. It is hard to guess the exact content of a quantum frame with an attacker.

In addition, the quantum verification algorithm is based on determining whether the special relationship transmitted data packet is quantum safe or not. By the non-ideal state this can change the behavior of sending packets to destroy special relationships and investigate random attack will reject the packet to send to the receiver, though the special relationship is broken.

Packets distributed in this form can always be moved toward the sink. So, if the opponent is only asking for direction from the source of the receiver, one possibility is that the pocket has taken other paths to stay safe and free from the black hole. These will send packets with backpressure routers and random nodes associated with the site.

Algorithm: Ideal Traffic Aware Routing

```
Initialize WSN Multi hop assigned nodes $M_n \rightarrow \{M_{ns1}, M_{ns2} \dots\}$
Compute Relational transmission path verification.
If (check route table == remain $M_{ns}$)
  Transmission begins
Else terminate route$\rightarrow T_l$
  Route Table $R_T \leftarrow T_l$ update
  Return Acknowledge root Node
End If
Compute the packet transmission $P_t$ on each relative link $RL$
Verify the distance routing on closes $t$ Node If node response
Neighbor relative weightage == access close node
Split the packets on Relay verification to pass the packet
For each packet on next hop verification speed terms on active
node
  For each referential $v_n$ as $tras_n$ node of $u_n$ response node:
    Sink destination Hop $\leftarrow$ reserve relay node [$u_n$] + length
    ($u_n$,$v_n$) packets
    Relay discovery compute closest node to non-related path $V$.
    If alt $\leftarrow$ reserve node [$v_n$]:
      Access node [$v_n$] $\leftarrow$ alternate path same $R_T \leftarrow$ begins
      Response verify the path at:
            Previous[$v_n$] $\leftarrow$ referential path $u$
      If relay node matches packet length same as
      acknowledgement access.
        If a particular packet itself is destined for the packet header
        then
          Check: Receive node
          Send the following node process data check
          If yes,
            Check if it has already received.
          Else
            Terminate access.
          End if
        End if
      End if
    End if
  End For
End for
```

The current node uses the current jam value to determine the next hop of the path. In this way, our packets are routed with less congestion and faster transmission and this will result in fewer packets. Traffic at a particular point in time, since different routes of a single node can be noticed from time to time.

4. RESULTS AND DISCUSSION

The reliable fast and ideal traffic aware secure routing protocol based on multi-hop cross site leaping for efficient packet transmission which is referred as (RTASR) The performance of further work on the NS2 simulator network is being evaluated under different simulation conditions. The results of the method were compared with the results of other methods.

Table.1. Throughput Comparative Result

Time (s)	FAEM	NPBNS	NSSR	RTASR
10	13	19	36	38
20	26	34	48	51
30	42	49	67	69
40	68	72	81	82
50	82	91	94	95

Functional performance has been measured at other times by an algorithm that is simulated and compared with the results of others. The RTASR method achieves a higher output rate than other methods in each simulation cycle.

The output performance introduced by the different methods is computed, and the results of Table.1, the comparisons are compiled by the RTASR method when the output is significantly higher than that proposed method.

The packet transfer rate generated by various strategies is measured by the number of packets sent and received. The packet transfer rates generated by them are measured and the results of other methods are compared.

Table.2. Performance on Packet Delivery Ratio (%)

Time (s)	FAEM	NPBNS	NSSR	RTASR
10	19	23	34	35
20	36	45	56	57
30	49	61	72	73
40	58	78	86	89
50	73	86	94	95

The rate of packet change is measured and the comparison is compared. Results in Table.2 shows the RTASR method obtains a higher PDR than other methods.

PDR performance is measured and the values of other methods are compared. Comparison indicates that the RTASR algorithm achieves higher PDR than previous methods. Delay is a measure of the time at which the packet is sent between any source and destination. Total time is measured based on the number of groups taken and the number of groups taken.

Table.3. Packet delay comparative result

Number of Packet/second	FAEM	NPBNS	NSSR	RTASR
4	4.5	3.4	1.8	1.9
8	6.8	4	2.9	2.3
16	7.2	6.5	4.3	3.6
32	8.9	7.1	5.9	5.1
64	9.4	8.9	6.4	5.4

Delays generated by various methods are calculated and presented. The algorithm presented in RTASR. The Table.3 produced shorter delays than other methods.

The Table.3 shows the different methods used, and the RTASR algorithm compares the latency delay rate with other methods that combine short-term values.

5. CONCLUSION

This projected method improves the security as well on fast transition with verifiable relay node to improve the WSN. Which is based on quantum transmission mechanism used to achieve data security in cross layer routing networks. This cross-site verification on packet transition verified the node to transfer the data, this used the adaptable quantum frame. Reliable fast and ideal traffic aware secure routing protocol based on multi-hop cross site leaping for efficient packet transmission in WSN can design inspection rules to check the transmission packet to make security n commination. When the status of the verification rule is satisfied, the receiver receives the transmission packet. Otherwise, the receiver will discard the data packet. Based on the above mechanism, data protection can be achieved and attacks carried out can be avoided with produce high performance.

REFERENCES

[1] Aykut Karakaya and Sedat Akleylek, “A Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks”, *Proceedings of 6th International Symposium on Digital Forensic and Security*, pp. 1-4, 2018.

[2] S.R. Rajeswari and V. Seenivasagarn, “Comparative Study on Various Authentication Protocols in Wireless Sensor Networks”, *The Scientific World Journal*, Vol. 2016, pp. 1-16, 2016.

[3] Yun Lin and Jie Chang, “Improving Wireless Network Security Based on Radio Fingerprinting”, *Proceedings of IEEE International Conference on Software Quality, Reliability and Security Companion*, pp. 1-5, 2019.

[4] X. Ye, X. Yin, X. Cai, A. Perez Yuste and H. Xu, “Neural-Network Assisted UE Localization Using Radio-Channel Fingerprints in LTE Networks”, *IEEE Access*, Vol. 5, pp. 12071-12087, 2017.

[5] Liang Huang, Xin Fan, Yan Huo, Chunqiang Hu, Yuqian Tian and Jin Qian, “A Novel Cooperative Jamming Scheme for Wireless Social Networks Without Known CSI”, *IEEE Access*, vol. 5, pp. 26476-26486, 2017.

[6] Nazli Siasi, Adel Aldalbahi and Mohammed A. Jasim, “Reliable Transmission Scheme against Security Attacks in Wireless Sensor Networks”, *IEEE Access*, Vol. 7, pp. 1-5, 2019.

[7] J. Ren, Y. Zhang, K. Zhang and X. Shen, “Adaptive and Channel Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks”, *IEEE Transactions on Wireless Communications*, Vol. 15, No. 5, pp. 1-15, 2016.

[8] E. Stavrou and A. Pitsillides, “WSN Operability during Persistent Attack Execution”, *Proceedings of International Conference on Telecommunications*, pp. 1-12, 2016.

[9] N.G. Palan, B.V. Barbadekar and S. Patil, “Low Energy Adaptive Clustering Hierarchy (LEACH) Protocol: A

Retrospective Analysis", *Proceedings of International Conference on Inventive Systems and Control*, pp. 1-8, 2017.

[10] Shailesh Pramod Bendale and Jayashree Rajesh Prasad, "Security Threats and Challenges in Future Mobile Wireless Networks", *Proceedings of International Conference on IEEE Global Conference on Wireless Computing and Networking*, pp. 146-150, 2018.

[11] Dongfeng Fang, Yi Qian and Rose Qingyang Hu, "Security for 5G Mobile Wireless Networks", *IEEE Access*, Vol. 6, pp. 4850-4874, 2018.

[12] Y. Ju, H. M. Wang, T.X. Zheng and Q. Yin, "Secure Transmission with Artificial Noise in Millimeter Wave Systems", *Proceedings of International Conference on IEEE Wireless Communications and Networking*, pp. 1-6 2016.

[13] N. Panwar, S. Sharma and A. K. Singh, "A Survey on 5G: The Next Generation of Mobile Communication", *Physical Communication*, Vol.18, No. 2, pp. 64-84, 2016.

[14] E. Dubrova, M. Naslund and G. Selander, "CRC-Based Message Authentication for 5G Mobile Technology", *Proceedings of International Conference on Trust, Security, and Privacy in Computing and Communications*, pp. 1186-1191, 2015.

[15] L. Wei, R. Q. Hu, Y. Qian and G. Wu, "Energy Efficiency and Spectrum Efficiency of Multihop Device-to-Device Communications Underlaying Cellular Networks", *IEEE Transactions on Vehicular Technology*, Vol. 65, No. 1, pp. 367-380, 2016.

[16] Haomeng Xie, Zheng Yan, "Data Collection for Security Measurement in Wireless Sensor Networks: A Survey", *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp. 1-22, 2018.

[17] G. Liu, Z. Yan and W. Pedryczc, "Data Collection for Attack Detection and Security Measurement in Mobile Ad Hoc Networks: A Survey", *Journal of Network and Computer Applications*, Vol. 105, pp. 105-122, 2018.

[18] H.Q. Lin, Z. Yan, Y. Chen and L.F. Zhang, "A Survey on Network Security-Related Data Collection Technologies", *IEEE Access*, Vol. 6, pp. 18345-18365, 2018.

[19] Y.F. Zheng, H.Y. Duan and C. Wang, "Learning the Truth Privately and Confidently: Encrypted Confidence-Aware Truth Discovery in Mobile Crowdsensing", *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 10, pp. 2475-2489, 2018.

[20] J. Ren, S. Member, Y. Zhang, K. Zhang and S. Member, "Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks", *IEEE Transaction on Wireless Communications*, Vol. 15, No. 5, pp. 3718-3731, 2016.