A Protocol Architecture for Trusted Underwater Acoustic Sensor Networks*

Zhengxian Wei [1,2]
[1]College of Computer Science and Technology Harbin Engineering University, Harbin, China
weizhengxian@sina.com

Min Song [3], Guisheng Yin[1], Yingqi Wang[1]
[2]System Engineering Research Institute, Beijing, China
[3]Beijing Foreign Studies University, Beijing, China

***Abstract*—Through adding the trusted protocol, trusted control and management mechanism on existing network architectures, a protocol architecture for trusted underwater acoustic sensor networks is presented, and the constitutes and functions of each part are described. The implementation model of trusted underwater acoustic sensor networks protocol is built, fundamental function that ensure the protocol can be executed as expected is defined, the functions and relationships between different layers of trusted protocol are given, considering the energy control and communication efficiency on the sensor networks, an example of dynamic clustering underwater target tracking network structure is designed in this paper.**

Keywords— sensor networks; acoustic; protocol; trustworthy; architecture

I. INTRODUCTION

In recent years, with the exploitation of the ocean resources all over the world, there are increasing needs for the research of the underwater acoustics communication network, the underwater monitoring system and the underwater acoustic warfare system[1]. As a result, the architecture and security of underwater acoustic sensor networks have become one of the research hotspots in the world. At present, to solve the network architecture and network security issues, the radio network technology often is referenced when designing the network architecture and protocol[2,3]. However, comparing with the radio transmitting channel, because of the narrow bandwidth and high transmission delay on the acoustics transmitting channel, and the energy limit on the sensor nodes, traditional radio network architecture and protocols can not be directly applied to underwater acoustic sensor networks[4]. Therefore, when we design the architecture and protocol of underwater acoustic sensor networks, the factors including acoustic communication delay, successful transmission ratio, data processing mechanism and network security should be considered, and a comprehensive integration solution must be given.

Underwater acoustic sensor networks are generally composed of sensor nodes and primary nodes in the sea, and the two-way acoustic communication system between them[5]. The acoustic communication system must be designed as a trusted network system, namely, the network behavior and its results can be expected and evaluated, the network status can be monitored, and network abnormal behavior can be controlled. Because of the narrow bandwidth, high transmission delay and energy limit on underwater acoustic sensor network, in order to make the energy control become more effective and the communication become more reliable, the network can work in a self organizing way, then the network topology has self-organization characteristic, the header node(HN) of the cluster is responsible for controlling network topology, at the same time is the data processing center. The other sensor nodes(SN) are responsible for collecting data and transmitting the data to the header node by means of the multi-hop or single-hop in the network. In order to save energy, reduce network traffic and keep the scalability, most sensor nodes only communicate with the header node in network, those sensor nodes are scheduled to communicating or sleeping under the control of the header node. So the network architecture and protocol must be suited those characteristics[6].

A network protocol architecture model includes the composition, functions, structures, relationships and processes, and more[7,8]. By adding trusted protocols, trusted control and management mechanisms on the existing network architecture, a network construction scheme is proposed in this paper, a reliable underwater acoustic sensor networks protocol framework is presented, the composition and function are described, and the key of achieving reliability is pointed out. Base on the above framework, through analyzing the function and process that ensure the protocol performs predictably, and defining the relationship of trusted protocols between different layers, the trustworthy implementation model of the underwater acoustic sensor network is given. Considering the energy control and communication efficiency on the sensor networks, a case of underwater acoustic sensor networks is designed in this paper, which shows that this network protocol architecture and trustworthy implementation model ensure the underwater acoustic sensor networks can return to the stable situation through self-diagnosis and self-recovery, and can be looked as guidance for building adaptive underwater acoustic sensor networks.

II. PROTOCOL FRAMEWORK OF TRUSTED UNDERWATER ACOUSTIC SENSOR NETWORK

A trusted underwater acoustic sensor network includes a set of attributes, from the user's view network security and survivability are needed, from design view the network should

This research is sponsored by the project of Science and Technology on Underwater Acoustic Antagonizing Laboratory and the Fundamental Research Funds for the Central Universities No. 2014JJ009.

be controllable. Under the goal of trustworthiness, the trusted network fuses three basic properties together through trusted maintain and behavior control to form integrated mechanisms.

Firstly, when the networks is disturbed by both internal and external factors, the network status and node behavior must be continuously monitored and analyzed, and the control parameters on nodes and its protocols must be adaptively optimized, then making the processing and result of data transmission, resource allocation and application services are to be expected. Secondly, the fault diagnosis tools and error information report channels must be provided, then give a meaningful feedback to network management. Thirdly, according to diagnosis results, the high level trusted adjustment strategies must be defined, then the network topology can be adaptively re-constructed or re-configured. This is three kinds of properties, which are called observable, controllable and accessible.

In order to enable underwater acoustic sensor networks to have above properties, based on the relatively mature sensor network protocol, through designing a set of trusted protocols, trusted control and management mechanism, then a trusted protocol framework is present in this section(Shown in Fig. 1).

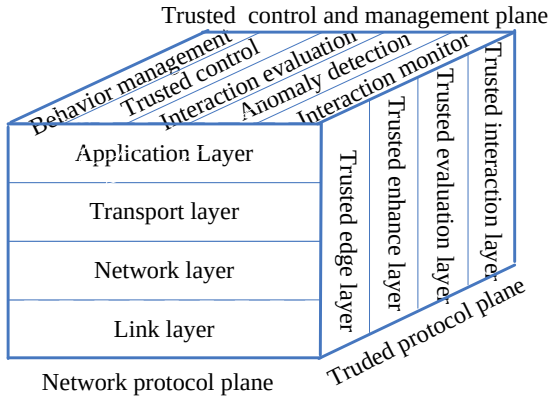

Fig. 1. Trusted underwater acoustic sensor network protocol framework

In Fig 1, the network protocol plane remains a mature underwater acoustic sensor network protocol at present, it is mainly responsible for carrying information transmission service for the network.

The trusted protocol plane includes a group of trusted protocols[9]. The trusted edge layer(TEdL) is responsible for monitoring trusty situation when the network behaviors interact based on the trusted protocols. Trusted enhancement layer(TEnL) locates in the core of protocol plane, and it can effectively improve trustworthiness of nodes when their behaviors interact each other in the network based on the trusted protocols. Trusted evaluation layer(TEvL) accurately evaluates the processing and results of protocol interaction. Trusted interaction layer(EInL) ensures trusted information be shared between network nodes.

Trusted control and management plane provides a group of consistent management mechanisms and control signals, it can control and coordinate the specific patterns of network behaviors. Interaction monitor mainly monitors the processing and status when the protocol runs. Anomaly detection can monitor and detect execution status of protocol. Interaction evaluation can effectively measure the result of protocol entity behavior. Trusted control need to prevent and kill the malicious behavior in the protocol entity. Behavior management should investigate responsibility of the behavior execution results, and stop anomaly behaviors.

Trusted control and management plane, trusted protocol plane extract “resource flow” and “trust flow” from the data stream which is transmitted in a network protocol plane. Through trusted protocol plane, trusted control and management plane, various states are apperceived during the running of a network, and the anomalies such as faults, Qos decreased, network attacks and node’s abnormal behaviors can be detected and identified timely, then according to present network status, and using game-based, voting, collaboration, competition and other means, the control measures are given. The credibility features of underwater acoustic sensor networks supported by this framework is that adaptively forming self-feedback network through ways such as monitoring, detecting, analysis, decision, control and so on.

III. IMPLEMENTATION MODEL OF TRUSTED UNDERWATER ACOUSTIC SENSOR NETWORK

The goal of trusted underwater acoustic sensor network protocol framework is to make sure those protocols can be running as expected. Therefore, the protocol framework must be able to achieve two functions, On the one hand, it has a reliable trust information source and real-time dynamic trusted analysis mechanism, which can ensure the reachability of the network behaviors, robustness of the trusted model and accessibility of the trusted information. On the other hand, it requires a controllable protocol implementation model to make the network controllable. The trusted underwater acoustic sensor network protocol framework aims to building a stable, reliable and coordinated network.

The processing of network protocol running includes interaction monitoring, anomaly detection, interaction evaluation, trusted control and behavior management, then we can design an implementation model of the trusted underwater acoustic sensor network protocol as shown in Fig 2. According to this model, the running process of network protocol is divided into five steps, which are specifically described as follows:

(1) In interaction monitoring step, the state of network running is real-time monitored, when the change on network status and node behavior are detected by the external disturbances, this change will be sent to the anomaly detection step.

(2) In anomaly detection step, according to the information from interaction monitoring step, and based on the trustworthiness of the historical behavior of nodes from the interaction evaluation step, the network behavior results and running status are synthetically analyzed, an observable panoramic trusted view about network status will be created and transmitted to interaction evaluation step.

(3) In interaction evaluation step, according to the observable panoramic trusted view from anomaly detection step, consistency analysis is carried out, including trustworthiness revaluation, situation evaluation, network warning, nodes voting and union-game, etc., and according to the consistency analysis results, the concrete control measure and scheme will be given, then transmitted to trusted control step.

(4) In trusted control step, the control measure and scheme will be run, including resource restructured, network reconfiguration and node isolation, etc., at the same time, the running status will be feedback to the interaction evaluation step.

(5) In behavior management step, the specific network topology will be dynamically adjusted to make the network return to a steady state, then build a closed-loop and self-adaptive network system.

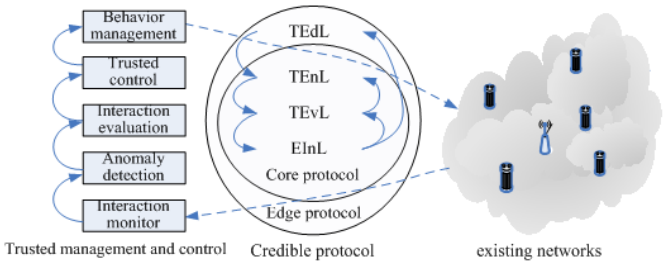

Fig. 2. Acoustic sensor network protocol implementation model

In order to ensure the protocol above steps availably run, trusted protocol layer agent entities need to be established respectively, making the functions such as perception and monitoring, understanding and detection, judgment and decision-making, control and manage can be executed respectively, the agent entities are described as follows:

(1) Trust edge layer entity is aware of the situation changes through monitoring the interactions data stream that existing trusted disturbance information, and then extracts trust flow that can be understood and detected by trust enhancement layer entity.

(2) Trust enhancement layer entity can understand and detect original trusted stream and historical trusted stream respectively come from the trusted edge layer entity and trust evaluation layer entity, then create a trust and transmit it to trust evaluation layer entity to make a decision. Specifically, according to trust stream in order to weed out the false "trusted data" which produced in trust interact, and stores the real trusted data to safely node, aiming at providing a visualization trusted view for trust evaluation layer entity.

(3) Trust evaluation layer entity evaluate the trustworthiness of trusted view and original feedback trusted stream respectively come from the trusted enhancement layer entity and trust interaction layer entity, and then the results are processed in two ways. The one is to provide trust control flows for trust interaction layer entity in order to control and process them. The other is to provide historical trust flows for trust enhancement layer entity in order to understand and detect them. Specifically, trusted evaluation layer entity searches out the trusted data form trusted view and original trust flow, uses the trusted evaluation engine to calculate trusted value after dealing with the strategy of oscillation guardian and trust information filtering. If the trusted value is not less than the trusted threshold, predict the trusted degree for the network behavior is predicted based on certain strategies. The processing result is either provided to trust interaction layer entity in a trust control flow way or fed back trust enhancement layer entity in a historical trust flow way.

(4) Trust interaction layer entity pushes the trust control stream into control and reachable processing program, and the results are processed in two ways. Firstly, the results are treated as control command impacting to network behavior interacting when the protocol executed with external disturbance. Secondly, the results are treated as original feedback trusted stream and fed back to trusted evaluation layer entity. Specifically, trust interaction layer entity analyzes the trusted control stream, then selects nodes and forms a controlled nodes set, and drives protocol executing. The processing of protocol execution is divided into two phases: pre-process phase and controllable execution phase. In the pre-process phase, the main task of trust interaction layer entity is to use a specific algorithms to derive "interactive proof" for this protocol execution circle, and make the members share them inner the controllable nodes set, the main purpose of this phase is ensure that the responsibility can be investigated after the execution.

In controllable execution phase, based on specifically trusted mechanisms, the specific network behaviors are interacted and the trusted protocols are executed between members inner the controllable nodes set, in this processing, the trusted interaction layer entity monitoring the state of behaviors interaction protocol execution through specifically strategy, and control anomalies actions according to some specific strategy. The results are divided into control command and original feedback trusted stream.

According above processing and entities function, implementation model of the trusted underwater acoustic sensor network protocol ensure the trusted data can be dynamically adjusted, so that trusted situation in the network can return to stability when the trusted protocols are executed, and trusted control processing can self-adaptively running in a closed-loop and feed-back cycle.

IV. TRUSTWORTHY UNDERWATER ACOUSTIC SENSOR NETWORK INSTANCE

Because of communication efficiency and energy limit on underwater acoustic sensor network, the network working as a cluster, and the cluster is serviced on data fusion, select routing and others basic function, so topology of cluster created based on trusted network protocol must meet requirements as follow.

(1) Underwater acoustic sensor network based on this trusted protocols must be able to maintain general network characteristics and performances, at the same time ensure the energy-efficiency of network topology to save the communication overhead among the cluster and energy cost.

(2) Trusted network sensor must have a reasonable communication overhead among the cluster and have a good scalaility.

According above trustworthy underwater acoustic sensor network protocol framework and its implementation model, a underwater target monitoring network(UTMN) as a typical application instance is designed in this section.

UTMN is composed by several data processing nodes(removable observation stations as master nodes--vessels) and lot of underwater acoustic modems(sensor nodes), it can self-organize into networks and be self-synchronization adjusted according to underwater environment changes when finding the target, the master nodes as removable observation station can maneuver to get a better position and angle for detecting and tracking the target, or they can choose to stay put and gather the detecting information by other nodes, and compute and analyze the target state. In the section, according the target position, the nodes of UTMN are dynamically organized to cluster, as show in Fig. 3, *r* is the largest communication distance of single-hop between nodes, *R* is the maximum effective detecting distance of nodes, *D* is the distance between cluster header node(HN) and the target.

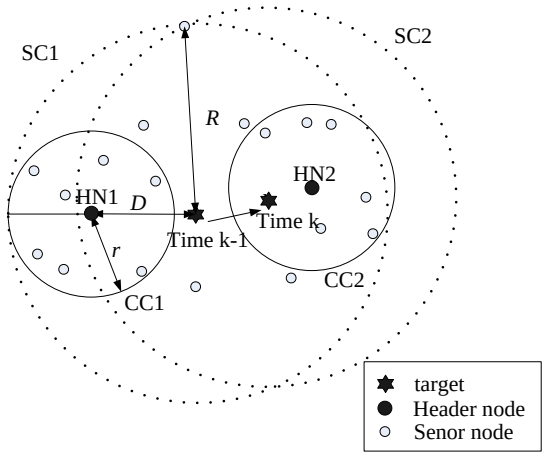

Fig. 3. Generating and removing of dynamic clustering

In the section, we assume that detecting radius *R* is much larger than the communications radius of single-hop *r*, the cluster is established that the *r* is the radius and NH is the center. In this cluster, the virtual line circle(SC) represent maximum effective detecting range of target, and its radius is *R*. The real line circle(CC) represent maximum single-hop communication range of HN, and its radius is *r*. The direct neighbor nodes are defined as the nodes whose distance is less than *r*. The communication between the direct neighbor nodes is implemented by single-hop.

All of nodes that distance less than *r* to HN are organized into a cluster, the HN processes the observations information to estimate target status within cluster. When $D+r<R$, the observations information to the target of all sensor child nodes(CN) is valid, there is no redundant nodes within cluster and the cluster is keeping. When $D+r>R$, the target is beyond the valid detecting scope of some CN in cluster, a new cluster necessary is created in order to effectively monitoring the target. There we can conclude the dynamic adjust processing of the cluster as follow.

$$\begin{cases} D+r<R & \text{Cluster is keeping} \\ D+r=R & \text{Translation critical of cluster} \\ D-r>R & \text{New cluster being created} \end{cases}$$

According UTMN characteristics and its dynamic cluster topology, energy limit in the removable observation stations can ignore, so the process of the trusted network is conducted in observation stations, and sensor nodes just take charge of trust certify and records trust history information. Before deploy nodes, each node is pre-loaded trusted mechanism sharing with the observation stations and authentication mechanism between neighbor nodes, and the observation stations also pre-loaded a random number for cluster header authentication and trusted mechanism for the whole network. Trustworthy and controllable network organization processing of dynamic clustering for UTMN is described by the following steps:

- Step 1: Network initialization. When the target moves into UTMN monitoring area, it will be detected and monitored, then the information such as target detected time, target azimuth, target feature and signal strength is encapsulated into a suite of data packets. Therefore the detected node can directly send these packets through single-hop communication way and establish paired-trust authentication with neighboring nodes, which could be used for message encryption and authentication between both nodes.
- Step 2: Trusted cluster-head selection. When the number of target nodes detected in the UTTN is exceeds a pre-determined threshold, at present, based on the strength of the received target signal and pre-loaded cluster-header authentication random number, the observation station closest to the target is selected as trusted HN.
- Step 3: Trusted notification and message broadcast from the cluster-head. HN broadcasts cluster-head authentication message and wake-up message to all nodes that are away from HN at most r distance, and collects historical trusted information for CN that has been working.
- Step 4: Confirmation of cluster-head by CN According to the pre-load node trusted mechanism and notification message that received from HN, CN confirms the HN identity, and retains its historical trusted information.
- Step 5: Secure clustering. The wakened CN sends the target monitoring information and the trusted information which is formed by trust mechanism to HN, the HN, as a data processing center, integrates the original monitoring data and local estimation data that are received from different CN together and generates state estimation for target tracking by specifically algorithm, at the same time produces clusters trusted

information and stores the historical trusted information.

- Step 6: Creation of a new cluster. With the movement of the target, the distance between HN and target meets with the critical condition of cluster transform. At that time the distance between CN and target is may be equal to the maximum effective detecting range--*R*, At the moment, through the target tracking algorithm and state estimation equation on current HN will predict target position in next sampling time point, and according the principle that closest this position, some new HN nodes are selected as a new cluster from newly detected target nodes. After loops the steps (2) to (5) until the cluster is created.
- Step 7: Trusted information transfer. The target state estimation and historical trusted information are gotten together and compressed into a data packet, and sent to the new HN from old HN, and make the other nodes into a sleeping state except the nodes in new cluster.
- Step 8: Over time, the dynamic clustering process has been done repeating until the target moves out the monitoring area of UTMN.

In UTMN, based on waken/sleeping mechanisms and trusted network protocol mechanisms on dynamically clustering, the dynamic trusted network topology can be established, then the energy consume of each node become more balanced, and because the trusted process mainly occur in the observation stations, then the sensor nodes energy consume among the sensor nodes is reduced. On the other, the monitoring and tracking data about target and trusted information are packaged together in a nodes within UTMN, the distance between HN and CN is less than single-hop communication distance, therefore the amount of communication data between nodes can be reduced and the node energy consume on CN using communication can be reduced dramatically.

V. CONCLUSION

At present, there are many security and trusted mechanisms of underwater acoustic sensor networks, but there isn't exist a set of rules which can unify these mechanisms effectively to realize the network highly safety and reliability, and be applied to underwater acoustic sensor networks. According to the characters of underwater acoustic sensor networks, it is urgent to need a new trustworthy architecture model. To achieve this goal, in this paper, through adding trusted protocols, trusted control and management mechanisms on existed networks architecture, a network construction scheme is proposed, Then a trustworthy underwater acoustic sensor networks protocol framework is presented, the compositions and functions are described, and the key of achieve reliable is pointed out. Base on this framework, we define the compositions and functions ensuring that the protocol execution can be predicted, and analyze relationships of trusted protocols between different layers, and give the trustworthy implementation model of underwater acoustic sensor networks is given. Considering the energy consumption and communication efficiency on the networks, a underwater target monitoring network with dynamically clustering as a example is designed, and it shows that the protocol framework and implementation model can ensure the underwater acoustic sensor networks can return to the stable situation through self-diagnosis and self-recovery, and can be looked as a guidance for building self-adaptive underwater acoustic sensor networks.

REFERENCES

[1] Sozer E M, Stojanovic M, Proakis J G, "Underwater Acoustic Networks," IEEE Journal of oceanic engineering. Vol.25, No.1, 2000, pp.72-83.

[2] Rice J, Creber B, Fletcher C, "Evolution of Seaweb underwater acoustic networking," OCEANS 2000 MTS/IEEE Conference and Exhibition. Vol.3, 2000, pp.2007-2017.

[3] Urick R J, "Principles of underwater sound," New York: McGraw-Hill, second edition. 1975, pp.35-46.

[4] LIN Chuang, LEI Lei, "Research on Next Generation Internet Architecture," CHINESE JOURNAL OF COMPUTERS. Vol.30, No.5, 2007, pp.694-711.

[5] Bavier A C, Feamster N, Huang M, Peterson L L, Rexford J, "In VINI veritas: Realistic and controlled network experimentation," Proceedings of the ACM SIGCOMM'06. Pisa, Italy, 2006, pp.3-14.

[6] Peng X, Lin C, "Architecture of trustworthy networks," Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. Indianapolis, Indiana, 2006, pp.269-276.

[7] LUO Jun-Zhou, HAN Zhi-Geng, "Trustworthy and Controllable Network Architecture and Protocol Framework," CHINESE JOURNAL OF COMPUTERS. Vol.32, No.3, 2009, pp.391-404.

[8] Bandyopadhyay S, Coyle EJ, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," In: Proc. of the IEEE INFOCOM. San Francisco: IEEE Computer Society, 2003, pp.1713-1723.

[9] YU Lei, LI Jian-Zhong, LUO Ji-Zhou, "Distributed Secure Clustering Protocol in Wireless Sensor Networks," Journal of Software. Vol.20, No.10, 2009, pp.2705-2720.