Security Issues of Wireless Sensor Networks Based on Target Tracking

Jun Ma

Luoyang Institute of Science and Technology, LuoYang, China

Abstract—**In this paper the dynamic point target tracking is studied, and a message driven target tracking algorithm based on non-ranging is proposed by combining the actual sensor node characteristics. By tissue tracking around the target sensor nodes collaborate to establish a tracking cluster and the cluster head node for data fusion to accurately locate the target and thus formed a kind of efficient and precise distributed dynamic tracking cluster algorithm of DTC. The tracking cluster can follow the target as a shadow, and it can realize the management of the cluster itself and constantly report to the sink node to the target location. The protocol is especially suitable for the use of large scale wireless sensor networks with low node cost.**

Index Terms—**WSN; Security; Optimization; Routing**

I. INTRODUCTION

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on[1].

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

Wireless sensor network target tracking problem, as it puts forward the earliest application requirements in military, scientific research, aerospace, medical, agriculture and animal husbandry, transportation and other applications have wide and important application prospect, and has been a research focus at home and abroad in recent years. Most of the existing target tracking protocols in wireless sensor networks focus on the improvement of the local performance of the network. Although people for the application of this technology in practice has put forward a lot of suggestions, but existing algorithms always exists a variety of defects that are less available for practical application in large-scale wireless sensor network system. Most of the existing algorithms are still in the experimental stage, often because they cannot meet the network size, security and other important indicators have become difficult to implement. In order to promote the development and practical application of wireless sensor networks, it is necessary to carry out in-depth research in this field [2].

II. RELATED WORK

Target tracking is one of the most important applications of wireless sensor networks can be widely used in the fields of transportation, security and battlefield reconnaissance, in recent years, people in the target tracking algorithms are a lot of research and achieved significant progress. Typical target tracking applications mainly include two types of target tracking and target tracking, the research on the application of wireless sensor network tracking is mainly focused on the point of target tracking. According to the implementation mechanism of the target tracking system, the research in the field of wireless sensor network is more influential in the target tracking algorithm mainly includes the following ways.

A. Dual element detection cooperative tracking

Sensor node has the characteristics of small size and low price, and its function is relatively weak. In the application of the target location, the general cheap sensors are difficult to accurately measure the distance, direction and properties of the target, so the most simple and intuitive target tracking sensor network is the dual detection target tracking[3].

Dual detection sensor cannot detect the distance of the node to the target, can only determine the target in the sensor detection range or outside of the two kinds of detection status. Because the target motion is random, it is very difficult to track the irregular trajectory. Dual detection method without affecting the tracking results under the conditions, assuming that the target within the detection range of the node uniform motion, thus the use of node location information to estimate the target location can approximate target trajectory as a broken line. Because the detection range of the single sensor node is

relatively small, the hypothesis is very close to the true trajectory of the target.

B. Message driven cooperative tracking

Collaborative tracking information driven sensor nodes use their detected information and received from other nodes detecting information judgment possible target trajectory, wake up the proper set of sensor nodes at the next moment in tracking activities. It not only requires sensor nodes to detect data processing, according to the different task demands and the limited resources selection of appropriate algorithms determine the target state, and the need to multiple nodes in the network work together, through the exchange of information to detect jointly determine the trajectory of the target, and the tracking results sent to network users. Sensor nodes can select the appropriate node to detect the target and transfer information through the exchange of information. Information driven collaborative tracking key is how through the exchange between the nodes of the tracking information on the trajectory of a moving object more accurate tracking, and the distributed autonomous algorithm can effectively reduce the amount of communication between nodes, which saves node limited energy resources and communication resources[4].

C. Convey-Tree

For a wide range of sensor units, a distributed target tracking algorithm using a transfer tree structure can be used. When the target is in the detection area, the sensor node of the target is detected first to select a root node, and the initial transmission tree is constructed. Each node periodically sends out the detection information and transmits it to the root node. The root node is collected to all the detection reports for data fusion processing, and the processing results are sent to the sink node. As the target moves, the transfer tree deletes the nodes that are farther and farther away from the target, and wakes up the node in the target moving direction to join the transmission tree. When the target distance from the root node exceeds a certain threshold value, the need to reelect the root node and re construct delivery tree[5].

The method of transmitting the root node by its own sensor unit to collect data and through local nodes exchange information for target tracking, and will change the tree structure as well as the moving target, dynamic additions and deletions to some nodes. The transmission tree structure is adapted to the sensor nodes with large sensor nodes, so that the node coverage area of the dynamic target is larger, and the moving speed of the corresponding target is low. Transfer root node update frequency is not too high, so in a relatively stable state, as long as the updated leaf node can guarantee delivery tree detection area coverage of the target, with respect to the information driven collaboration tracking can significantly reduce the cluster update frequency.

This algorithm provides a feasible method for the application of the sensor networks in the field of target tracking, and further reduces the reconstruction frequency to reduce the energy consumption. But most of the existing sensor nodes, the node communication distance is far greater than the sensing distance, the algorithm in the actual application performance still needs further research.

D. Face target tracking algorithm

Sensor network tracking, in many cases, the need to track a larger area of the target, such as forest fires in the edge of the advancing path, the path of the typhoon, etc. In this case only by the collaboration of the local node cannot detect the complete trajectory of the target. Therefore some scholars proposed using dual space transformation method, that determines which nodes are involved in tracking, to ensure that the trajectory of moving target detection[6].

E. Wireless sensor networks Trust Management Categories

Hierarchical trust management is the assessment of the trust and other values, and pass a hierarchical storage management features, often with the application of network topology and confidence values are closely linked. Data security; if the base station and sensor nodes based on natural hierarchy formed by the base station as the center of trust management; - - cluster head node ordinary nodes of layer 3 of trust in management there is a cluster structure of a sensor network, the base station will form aggregation applications, often based on trust management aggregation tree hierarchy. In the hierarchical trust management, the trust can pass layer by layer, the higher the value of the trust store all subordinate or subordinates adjacent. Trust can also be progressively converge, forming different levels of trust value. Planar trust management is the process of trust management, the network status of all nodes and base stations are equal, take the same model and management strategies, there is no obvious or central level.

1) Global trust management and trust management local.

Global trust management means that a node has a unique trust value across the entire network, the general common sensor network cluster structure. Local trust management refers to the node being evaluated to assess different values may be inconsistent trust at the node in the node to make decisions based on trust value stored locally or transmitted credibility comprehensive decision based on local trust value and neighbors.

2) Trust management based on trust and credibility of local management based on information collection.

When conducting trust evaluation because of incomplete information may cause deviation of the assessed value, in order to obtain a more accurate value of the trust, the trust often need to consider the assessed value of the other node to correct local assessment results, which is based on the credibility of the trust management the basic idea. But in the sensor network, node due to limited resources, to reduce the cost of communication and computing, and some trust management system in the assessment of the value of trust, simply consider the node itself to be observed and the results of the assessment node interactions evaluation local information, save other transport node reputation value of energy consumption.

3) General trust management and trust management related applications.

General Trust management is considering all aspects of trust defined element of the definition of a complete trust management framework, including information collection, transmission, storage trust management, calculation, up-

date other aspects of the design. Calculated trust value untargeted, is a comprehensive assessment of the credibility of the nodes, sensor networks can be used to run applications and all related technologies. And the application of the relevant trust management are well targeted, trust management of all aspects of the design process are closely associated with a particular application, such as trust management often need to identify safe routes selfish nodes, low competitiveness node, and for secure data fusion trust management selfish nodes generally do not need treatment, even in some systems, when a malicious node does not send the error data will not affect the value of their trust.

III. MULTI NODE COOPERATIVE TARGET TRACKING ALGORITHM

Usually a target's appearance will be detected around a certain range of sensor nodes, which are usually adjacent to each other. At this time through the organization of these locations related to the local collaboration, to locate the target is an effective and intuitive way of. Through the cooperation of these nodes[7], the local node tracking data fusion can effectively reduce the data communication between nodes in the premise of ensuring the accuracy of tracking, thus saving the node energy and communication bandwidth. The key of the cooperative tracking is how to realize the accurate tracking of the target trajectory through the exchange of information between nodes, while minimizing the energy consumption of the node. Key issues of collaborative tracking include determining which nodes are to be tracked, which need to be acquired and what information must be exchanged between the nodes. Considering the node is needed to obtain a tracking information validity, accuracy and node complete tracking task requires the energy cost, in order to determine which sensor nodes should be involved in the tracking process and tracking node collaboration.

In this paper, based on the principle of multi point cooperative target tracking, a dynamic tracking cluster protocol DTC is proposed, which is based on the performance of the existing sensor nodes. In this paper, we use R to represent the effective communication radius of nodes, and R indicates the effective sensing radius of the sensor nodes. We note that the communication transmission distance of the existing sensor nodes is usually far away (R>loom), while the traditional sensor devices are relatively short (<40m), such as sound, magnetic and other sensors. So different from the traditional message driven, tracking tree algorithm, DTC protocol is mainly aimed at low cost wireless sensor nodes used in large scale network design[8].

In this paper, we make the following assumptions: sensor network nodes know their location information; network overall in each element are equipped with sensors that can detect targets, but these sensors function is weak only to judge whether the target is, cannot judge the direction and distance; nodes in a certain extent synchronization; each sensor only in the distance in half the distance of wireless communication range of the target tracking, which also limits the simultaneous sensing to the distance between the two sensors in a target are in each other.

IV. DTC ALGORITHM

Target tracking wireless sensor networks are usually large-scale random spread, and the whole network is a kind of unstructured planar network. Each node in the network is peer to peer, it is likely to become cluster head node. In order to describe the dynamic tracking cluster algorithm DTC, a finite automaton model is used to describe the state of each sensor node in the target tracking process[9].

Routing path of delay and energy consumption, and the number of AP on the routing path, each AP asked to lie off the tight phase, in fact, is how to set the distance between the various sectors of the base station, that is, how to select the ring size. The energy consumption of the routing is also related to the sector size and the distance from the base station of each sector. The nearest ring starting from the tomb station is in turn.:r1,r2,...,rk.: For r1, for the R1 assuming a bit transmission of this distance of energy consumption for the Cr12, then, for the Aj to Aj-1, it is easy to get its value of c(rj-rj-1)2. This set of r0=0, the path from the sector Ai to the base station for the energy consumption of the routing path:

$$E_i = c \sum_{j=1}^{i} (r_j - r_{j-1})^2 \tag{1}$$

introduced the following:

$$\sum_{1 \le p < q \le i} (a_p b_q - a_q b_p)^2 = \sum_{p=1}^{i} a_p^2 \sum_{p=1}^{i} b_p^2 - (\sum_{p=1}^{i} a_p b_p)^2 \tag{2}$$

(1) into the(2) type, you can get:

$$E_i = \frac{c}{i}(r_i^2 + \sum_{1 \le p < q \le i} (a_p - a_q)^2) \tag{3}$$

It is obvious that the (3) type left is the smallest and must be made:

$$\sum_{1 \le p < q \le i} (a_p - a_q)^2 = 0 \tag{4}$$

For (4) - type when and only if:

$$a_1 = a_2 = a_3 = ... = a_4 \tag{5}$$

Form(4) and(5),we can get:

$$E_i = icd^2 \tag{6}$$

Let tx for the maximum transmission radius of AP, and set up d=tx:

$$E_i = i(ct_x^2) \tag{7}$$

From the (7) type, it is known that the minimum energy consumption of the base station must be equal to the distance between each ring, and the distance is the maximum transmission distance of AP.

V. TEST AND ANALYSIS

In order to test the performance of the protocol, we select the Ns2(network simulator 2) as a simulation tool to test the DTC protocol.

Ns began as a variant of the REAL network simulator in 1989 and has evolved substantially over the past few years. In 1995 ns development was supported by DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. Currently ns development is support through DARPA with SAMAN and through NSF with CONSER, both in collaboration with other researchers including ACIRI. Ns has always included substantial contributions from other researchers, including wireless code from the UCB Daedelus and CMU Monarch projects

and Sun Microsystems. Ns2 is a discrete event simulator for network research, which can be easily used to simulate all kinds of wireless network protocols and network architecture by adding CMU wireless extension[10].

Experiment uses 20 MicaZ nodes, which are divided into 10 groups. Each group has two nodes: respectively, sending node and receiving node. And do the following requirements: 1 The Micaz node connected with base stations as receiver named node A; The Micaz node which send data to node A named node B. From above test: In the same distance, the relationship between packet reception ratio and the distance for forward link and reverse link.

In the following experiments, we randomly placed 100 nodes to monitor the temperature at 140 m * 40 m in the sensing area, and investigate the accuracy of the probability and data acquisition results of the safety election cluster heads[11].

Neighbor nodes monitor each other, determine each other's trust value, and submit their most trusted neighbor nodes as candidate cluster heads in each cluster head election. In the presence of malicious nodes, they may cheat the neighbor's trust to become the candidate cluster head, Figure 1 shows the probability that the node in our program will be malicious neighbors selected as candidate cluster heads. As shown in the Figure 2, the probability of a malicious node to become the candidate cluster heads is very small, and it has little effect on the correct candidate cluster head, and decreases with the decrease of the captured rate.

In order to influence degree of agreement on DTC by the speed of the test target, we make the target node from the origin through the same path mobile point-to-point (1000·1000) site at different speeds. From 16 of the test results shown in Figure 3, the target speed is slower, the more effective tracking data. This is caused by two reasons:

1. When the target is low speed, the retention time in the network is longer;
2. The frequency of the cluster update is low, the effective working hours of a single cluster is longer. Because the cluster update is triggered by the distance between the target and the cluster head, the data of the control packets used for cluster update is not large.

When the target moves at a speed of over 40, which is 144KM/H, the proportion of effective tracking results is reduced due to frequent cluster update, which makes the cluster update cost increased.

Tests show that the DTC protocol can effectively track the moving target in the coverage area of wireless sensor networks.

Table 1 shows the change of the trust value of the member nodes stored in the cluster head. In the protocol of our design, the initial trust value of the nodes is 1, and the value of trust is gradually changing with the cluster head. The overall trend is that the trust value of malicious nodes decreases, and the trust value of normal nodes is close to 1. As is shown in Figure 4, the variation of the curve verifies the correctness of the protocol.
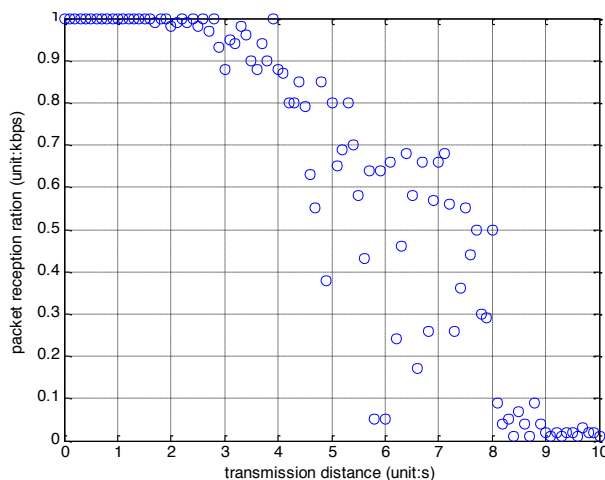

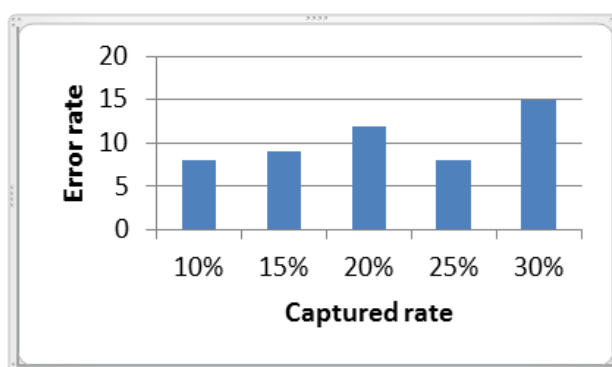Figure 1. The relationship between d and prr from A to B
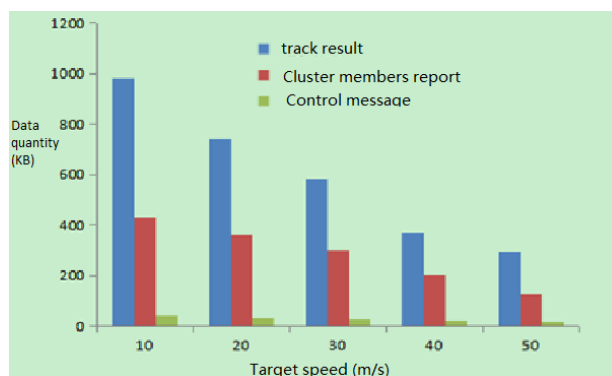

Figure 2. Error rate of node

Figure 3. Effect of target speed on DTC

TABLE I.
PROBABILITY OF SELECTING COMPROMISED NODES AS CLUSTER HEAD

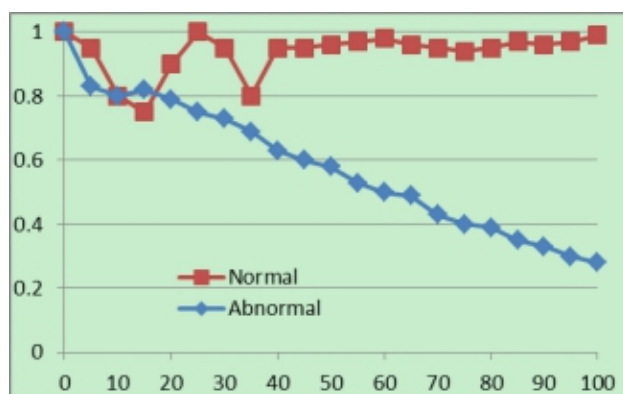| Compromised node ratio(%)	Probability(Using trust grid head election)	Probability(without trust mechanism)
0	0	0
15	0	0.2
50	0.1	0.4
85	0.2	0.8
100	1	1

Figure 4.   Trust value of node

VI.   CONCLUSION

In this paper, we propose a distributed dynamic tracking cluster algorithm DTC. The algorithm is based on the condition of large scale spread of cheap sensor nodes, which is consistent with the design requirements of wireless sensor networks. By tissue tracking sensor nodes around the target, this protocol can is achieved at the expense of its cluster maintenance and update of consuming in communication with the computing capability of cluster head node, and through using the improved algorithm of convex programming to the intra cluster data fusion, elimination of redundant data and accurately locate the target. The algorithm mainly considers the case that the sensor radius of the node is less than half of the transmission radius, that is, $r<R/2$. In line with the actual situation of the current sensor network. Simulation results show that the proposed protocol can efficiently and accurately track the moving target, and has practical application value.

REFERENCES

[1] Syed Hashim Raza Bukhari; Mubashir Husain Rehmani; Sajid Siraj, A Survey of Channel Bonding for Wireless Networks and Guidelines of Channel Bonding for Futuristic Cognitive Radio Sensor Networks[J],IEEE Communications Surveys & Tutorials, Year: 2016, Volume: 18, Issue: 2 Pages: 924 - 948..

[2] Yulong Zou; Gongpu Wang, Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack[J], IEEE Transactions on Industrial Informatics, Year: 2016, Volume: 12, Issue: 2.Pages: 780 - 787..

[3] Syed Hashim Raza Bukhari, A Survey of Channel Bonding for Wireless Networks and Guidelines of Channel Bonding for Futuristic Cognitive Radio Sensor Networks. IEEE Communications Surveys & Tutorials[J].2015.11.30,page(s):924-948.

[4] Xinheng Wang, Scalable Routing Modeling for Wireless Ad Hoc Networks by Using Polychromatic Sets. IEEE Systems Journal[J], 2012.10.11, page(s):50-58

[5] Ning Wang; Yong Zhu; Wei Wei; Jianjun Chen; Shenshen Liu; Ping Li; Yumei Wen, One-to-Multipoint Laser Remote Power Supply System for Wireless Sensor Networks[J],IEEE Sensors Journal, Year: 2012, Volume: 12, Issue: 2, Pages: 389 - 396.

[6] Haiying Shen, A Scalable and Mobility-Resilient Data Search System for Large-Scale Mobile Wireless Networks ,IEEE Transactions on Parallel and Distributed Systems[J].2013.7.16.page(s):1124-1134.

[7] Hossein Fotouhi; Reliable and Fast Hand-Offs in Low-Power Wireless Networks. IEEE Transactions on Mobile Computing[J].2014.02.24.page(s):2620-2633.

[8] Ruonan Zhang, A hybrid reservation/contention-based MAC for video streaming over wireless networks. IEEE Journal on Selected Areas in Communications[J].201004.11.page(s):389-398.

[9] Arslan Munir; Ann Gordon-Ross; Sanjay Ranka, Multi-Core Embedded Wireless Sensor Networks: Architecture and Applications[J].IEEE Transactions on Parallel and Distributed Systems, Year: 2014, Volume: 25, Issue: 6,Pages: 1553 - 1562..

[10] Jae-Hyun Park, All-Terminal Reliability Analysis of Wireless Networks of Redundant Radio Modules, IEEE Internet of Things Journal[J].2016.03.23.page(s):219-230

[11] JongHyup Lee; LeeHyung Kim; Taekyoung Kwon, FlexiCast: Energy-Efficient Software Integrity Checks to Build Secure Industrial Wireless Active Sensor Networks[J],IEEE Transactions on Industrial Informatics, Year: 2016, Volume: 12, Issue: 1,Pages: 6-14..

AUTHOR

MA Jun is with Department of Economics and Business Administration, Luoyang Institute of Science and Technology, LuoYang, China (e-mail: mj@lit. edu.cn).